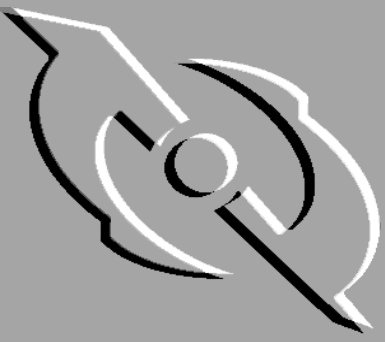


VirusScan for Windows NT

User's Guide

Version 4.0

COPYRIGHT

Copyright © 1998-1999 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 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.

10. **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.

11. **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.

12. **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

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 40,000 known viruses in circulation capable of attacking Windows- and DOS-based computer systems, it really is only a matter of time before you do.

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

Why worry?

So why worry about virus infections, if most attacks do little harm? The problem is twofold. First, although relatively few viruses have destructive effects, that fact says nothing about how widespread the malicious viruses are. In many cases, viruses with the most debilitating effects are the hardest to detect—the virus programmer bent on causing harm will take extra steps to avoid discovery. Second, even "benign" viruses can interfere with the normal operation of your computer and can cause unpredictable behavior in other software. Some viruses contain bugs, poorly written code, or other problems severe enough to cause crashes when they run. Other times, legitimate software has problems running when a virus has, intentionally or otherwise, altered system parameters or other aspects of the computing environment. Tracking down the source of resulting system freezes or crashes 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. Some estimates have placed the total worldwide cost in time and lost productivity for merely 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 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. As further catalyst, virus writers found it relatively easy to exploit some PC technologies to serve their own ends.

Boot-sector viruses

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

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

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

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

But 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 other vendors, 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. But most existing anti-virus software easily kept pace with updates that detected and disposed of the new virus variants, which consisted primarily of minor tweaks to well-known templates.

But 1995 marked the emergence of the Concept virus, which added a new and surprising twist to virus history. Before Concept, most virus researchers thought of data files—the text, spreadsheet, or drawing documents created by the software you use—as immune to infection. Viruses, after all, are programs and, as such, needed to 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, the flagship applications in its Office suite. Using the stripped-down version of its Visual BASIC language included with the suite, users could create document templates that would automatically format and add other features to documents created with Word and Excel. 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.

Where next?

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. The chat client sends script viruses as plain text, which would ordinarily preclude them from infecting systems, but older versions of the mIRC client software would interpret the instructions coded into the script and perform unwanted actions on the recipient's computer. The vendors moved quickly to disable this capability in updated versions of the software, but the mIRC incident illustrates the general rule that where a way exists to exploit a software security hole, someone will find it and use it.

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. Anti-virus software, moreover, is only as good as its latest update. Because as many as 200 to 300 viruses and variants appear each month, the data (.DAT) files that enable Network Associates software to detect and remove viruses can get quickly outdated. If you have not updated the files that originally came with your software, you could risk infection from newly emerging viruses. Because Network Associates has assembled the world's largest and most experienced anti-virus research staff within its McAfee Labs division, however, the updated files you need to combat new viruses appear as soon as—and often before—you need them.

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

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 your 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.

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, 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.
McCandless Towers
3965 Freedom Circle
Santa Clara, CA 95054-1203
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 Response System	(408) 988-3034
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
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- 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 anti-virus product documentation to: Network Associates, Inc., 15220 NW Greenbrier Parkway, Suite 100, Beaverton, OR 97006-5762, U.S.A. You can also send faxed comments to (503) 531-7655 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 Java classes, ActiveX controls, dangerous websites, or 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 questions or virus samples to:

virus_research@nai.com	Use this address to send questions or virus samples to our North America and South America offices
vsample@nai.com	Use this address to send questions or virus samples gathered with Dr Solomon's Anti-Virus Toolkit software to our offices in the United Kingdom

To report items to our European research offices, use these e-mail addresses:

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

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

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

International contact information

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

Network Associates Australia

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

Network Associates Austria

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

Network Associates Belgium

Bessenveldtstraat 25a
Diegem
Belgium - 1831
Phone: 32-2-716-4070
Fax: 32-2-716-4770

Network Associates do Brasil

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

Network Associates Canada

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

Network Associates People's Republic of China

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

NA Network Associates Oy

Sinikalliontie 9, 3rd Floor
02630 Espoo
Finland
Phone: 358 9 5270 70
Fax: 358 9 5270 7100

Network Associates France S.A.

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

Network Associates Deutschland GmbH

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

Network Associates Hong Kong

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

Network Associates Srl

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

Network Associates Japan, Inc.

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

Network Associates
Latin America

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

Network Associates
de Mexico

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

Network Associates
International B.V.

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

Network Associates
Portugal

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

Net Tools Network Associates
South Africa

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

Network Associates
South East Asia

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

Network Associates
Spain

Orense 4, 4ª Planta.
Edificio Trieste
28020 Madrid
Spain
Phone: 34 91 598 18 00
Fax: 34 91 556 14 04

Network Associates
Sweden

Datavägen 3A
Box 596
S-175 26 Järfälla
Sweden
Phone: 46 (0) 8 580 88 400
Fax: 46 (0) 8 580 88 405

Network Associates AG

Baeulerwisenstrasse 3
8152 Glattbrugg
Switzerland
Phone: 0041 1 808 99 66
Fax: 0041 1 808 99 77

Network Associates International Ltd.

Minton Place, Victoria Street
Windsor, Berkshire
SL4 1EG
United Kingdom
Phone: 44 (0)1753 827 500
Fax: 44 (0)1753 827 520

Network Associates Taiwan

Suite 6, 11F, No. 188, Sec. 5
Nan King E. Rd.
Taipei, Taiwan, Republic of China
Phone: 886-2-27-474-8800
Fax: 886-2-27-635-5864

Introducing VirusScan 1

What is VirusScan?

VirusScan for Windows NT is a key desktop element in the Network Associates Total Virus Defense suite of security tools. Its powerful scanning technologies permit it to act as a tireless online sentry, guarding your Windows NT workstations against attacks from viruses and preventing harm from other malicious software.

Because networked computing and the emergence of collaborative technologies have dramatically increased the speed at which viruses spread in the corporate workplace, taking precautions against malicious software is no longer a luxury, but a necessity. Consider the extent to which you rely on the data on your computer and the time, trouble and money it would take to replace that data if it became corrupted or unusable because of a virus infection. Balance that possibility against the time and effort it takes to put a few common sense security measures in place, and you can quickly see the utility in protecting yourself against infection.

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

VirusScan gives you the tools you need to keep your system intact and secure. Used properly as one part of a comprehensive security program that includes backups, meaningful password protection, training, and awareness, VirusScan can keep your computer safe from debilitating attacks and prevent the spread of malicious software throughout your network.

What comes with VirusScan?

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

- **Common Components.** This component set consists of data files and other support files that many of the VirusScan component programs share. These files include VirusScan virus definition (.DAT) files, default configuration files, validation files, and other files.

- **VirusScan AntiVirus Console.** This component is your primary VirusScan interface. You can use the Console to create, configure and schedule scan tasks, update your virus definition files and program components, and configure VirusScan's on-access scanning component. The Console comes with a preconfigured set of tasks for updating virus definition files and program components, and an on-access task monitor that allows you to configure VirusScan's background scanning function. You can create new scan tasks either with a Scan Wizard, or with a series of property pages. To learn how to start and use the Console, see Chapter 3, "Getting Started."

- **VirusScan on-demand scanner (SCAN32.EXE).** This component lets you initiate an immediate scanning operation at any time—a feature known as "on-demand" scanning. You can start it independently of the AntiVirus Console and use it to specify local and network disks as scan targets, choose how to respond to any infections it finds, and see reports on its actions. When you schedule a scan operation through the AntiVirus Console, the Network Associates Task Manager starts this component to perform the scan operation. To learn how to configure on-demand scan operations, See "Using McAfee VirusScan" on page 123.

- **Network Associates McShield.** This Windows NT service is VirusScan's on-access scanning component. It operates as a background process, watching for activity on your workstation or on network drives you have mapped to your system. Each time you or another user opens, copies, saves, or otherwise makes use of any file on your system, VirusScan searches that file for viruses.

  You can configure the service from the VirusScan On-Access Monitor in the AntiVirus Console. You can also enable and disable this service from the Windows NT Services control panel. Network Associates recommends, however, that you control this service from the AntiVirus Console unless specific circumstances require you to disable it from the control panel.

- **Network Associates Task Manager.** This Windows NT service runs any scan operations you schedule for later execution. It, like the Network Associates McShield service, operates as a background process, which frees you from the need to keep the AntiVirus Console running in order to run scheduled tasks.

  This service begins running as soon as you install and reboot your workstation. You can enable and disable this service from the Windows NT Services control panel, but Network Associates recommends that you leave it enabled unless specific circumstances require you to control it from the Windows NT control panel.

- **Alert Manager.** This Windows NT service receives and distributes alert messages that warn you or other users when VirusScan has detected a virus. Alert Manager provides you with 10 different ways to send alert messages, and includes a flexible configuration utility that allows you to specify delivery options. As the other Network Associates services do, the Alert Manager service operates as a background process that you can control from the Windows NT Services control panel.
- **File Copy utility.** This utility enables VirusScan's AutoUpdate and AutoUpgrade utility to log on to and retrieve .DAT file updates and program component upgrades from NetWare servers on your network. If you use a NetWare server as a central distribution point for VirusScan files, you should install this utility as part of a custom installation—VirusScan's Setup utility does not install it by default.
- **Documentation.** VirusScan documentation includes:
  - A *Getting Started Guide*, which introduces the product, provides installation instructions, outlines how to respond if you suspect your computer has a virus, and provides a brief product overview.
  - This user's guide saved on the VirusScan CD-ROM or installed on your hard disk in Adobe Acrobat .PDF format. The VirusScan *User's Guide* describes in detail how to use VirusScan and includes other information useful as background or as advanced configuration options. Acrobat .PDF files are flexible online documents that contain hyperlinks, outlines and other aids for easy navigation and information retrieval.

    You can also download the User's Guide from the Network Associates website at:

    ftp://ftp.nai.com/pub/manuals/total_virus_defense/_english_us
  - An online help file. This file gives you quick access to hints and tips about how to use VirusScan. To open the help file from within VirusScan or from within VirusScan Scheduler, choose **Help Topics** from the **Help** menu.

    VirusScan also includes context-sensitive online help. Right-click buttons, lists or other elements within dialog boxes to see brief, descriptive help topics. Click **Help** buttons where you see them to open the main help file to a relevant topic.
  - A README.1ST or LICENSE.TXT file. This file outlines the terms of your license to use VirusScan. Read it carefully—if you install VirusScan you automatically agree to its terms.

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

VirusScan Features

- New-generation Network Associates scanning technology gives VirusScan the ability to detect and remove more than 40,000 known file, macro, multi-partite, stealth, encrypted and polymorphic viruses.
- Network Associates anti-virus researchers provide fast, responsive coverage for new viruses and other malicious software. A preeminent, worldwide staff made up of the former McAfee and Dr Solomon teams develops and backs each new scan engine update and virus definition file release.
- On-access scanning capability lets VirusScan look for viruses whenever you create, open, save, run, or copy files over your network.
- Powerful on-demand scan modules let you start a scan operation immediately or schedule regular scan operations that suit your work flow.
- Advanced heuristic scanning technology detects previously unidentified or unclassified macro viruses.
- Flexible alerting methods can automatically notify you when VirusScan finds a virus, while automated responses ensure that you can clean, isolate, or delete the infected file; and record the results in a log file for later review.
- Scan task creation is quick and easy with VirusScan's intuitive Scan Wizard.
- Automatic, scheduled virus definition updates and program component upgrades can ensure that VirusScan has up-to-the-minute scanning technology to deal with viruses as they emerge from the field. Update from an FTP site or a designated server on your network to ensure complete control over your anti-virus security measures.

Deciding when to scan for viruses

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

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

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

Even the most diligent scan operation can miss new viruses, however, if your scanning software is not up to date. Your VirusScan purchase entitles you to free virus updates for the life of your product, so you can update frequently to keep current. See “Configuring AutoUpdate options” on page 173 to learn how to update your virus definition files and VirusScan program components.

Recognizing when you don’t have a virus

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

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

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

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

Installing VirusScan 2

Overview

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

Before you start

To install VirusScan, you must have Administrator privileges for the local or remote workstation on which you plan to install the program, and you must have logged on to that system correctly. Review the system requirements shown below to determine whether your target workstations can run VirusScan.

System requirements

NOTE: Much of VirusScan consists of Windows NT services. Your workstation does not need additional memory to run these services, but the amount of system resources they require can vary. If you specify a scanning priority for each task, you can determine what system resources the program uses.

VirusScan for Windows NT will install and run on a local or a remote workstation equipped with:

- An Intel processor or a compatible architecture, or a DEC Alpha processor
- Windows NT version 3.51 or later

IMPORTANT: Do not attempt to install the VirusScan version optimized for Intel-architecture workstations on a DEC Alpha system, and do not attempt to install the VirusScan version optimized for Alpha-architecture workstations on workstations with Intel or compatible processors.

- Windows NT v3.51 Service Pack 5 (required) or Windows NT v4.0 Service Pack 4 (recommended)
- At least 6MB of free disk space on your local workstation. Remote workstations will usually require less disk space.

Installing VirusScan on a local workstation

To install VirusScan on your local workstation, you must use a Windows NT account with Administrator rights. First log on to your system, then follow the installation steps outlined below.

Installation Steps

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

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

  IMPORTANT: If you suspect that your computer has a virus infection, download the VirusScan installation files onto a computer that is ***not*** infected.

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

If you inserted a CD-ROM disc, you should see a VirusScan welcome image appear automatically.

Follow these steps:

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

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

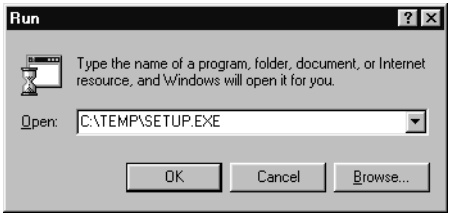


Figure 2-1. Run dialog box

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 VirusScan files. To search for the correct files on your hard disk or CD-ROM disc, click **Browse**.

NOTE: If your VirusScan copy came on a VirusScan Security Suite or a Total Virus Defense CD-ROM disc, you must also specify which folder contains VirusScan for Windows NT. To learn where to find the correct folder, see the CONTENTS.TXT file included with either CD-ROM disc.

Setup will start and display its welcome panel (Figure 2-2).

Figure 2-2. Welcome to Setup wizard panel

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

   The next wizard panel displays the VirusScan end-user license agreement. Read this agreement carefully—if you install VirusScan, 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.

5. Setup asks you whether you want to install VirusScan on your local workstation or on other computers elsewhere on your network (see Figure 2-3 on page 34). Click **Local Installation**, then click **Next>**.

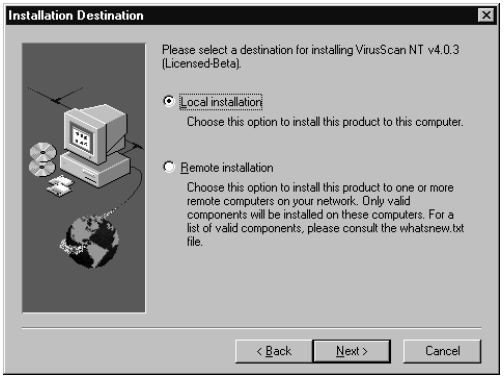


Figure 2-3. Installation Destination panel

If Setup detects an existing version of VirusScan for Windows NT v3.1.4a or later, it will offer to remove it completely from your computer or to remove the software but preserve your existing configuration options (Figure 2-4).

If Setup finds an existing version of VirusScan for Windows NT earlier than v3.1.4a, or an existing version of Dr Solomon Anti-Virus Toolkit v7.74 or later, it will offer only to remove that version from your system.

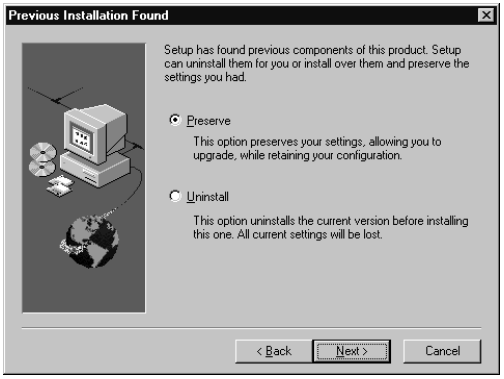


Figure 2-4. Previous Installation Found panel

6. To continue, you can 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.

When it finishes removing earlier software, Setup will display the Setup Type panel (Figure 2-5).

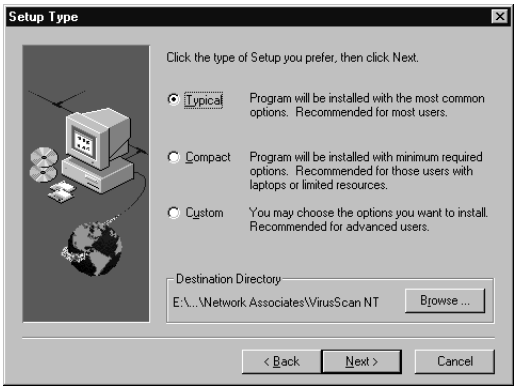


Figure 2-5. Setup Type panel

7. Select the VirusScan component sets that you want to install. You can choose from these options:

   - **Typical.** Select this option to install the VirusScan AntiVirus Console, the VirusScan on access and on-demand scanners, the Network Associates Task Manager service, and the Network Associates Alert Manager service. This component set will suit most users' needs.
   - **Compact.** Select this option to install the AntiVirus Console and the Network Associates Task Manager service. This will allow you to schedule and initiate on-demand scan operations only. Network Associates recommends this option only if you have minimal free disk space or other system constraints.
   - **Custom.** Select this option to choose which VirusScan components you want to install. By default, the Custom option installs most of the same components as the Typical installation, but you can also choose to install a file copy utility that works with the Automatic DAT Update and the Automatic Product Upgrade utilities to download files from NetWare servers.

     IMPORTANT: Do *not* install the file copy utility on your system unless you use NetWare servers to distribute virus definition updates and product upgrades. If you do not have a network environment with this configuration, the file copy utility can misdirect the Automatic DAT Update and Automatic Product Upgrade utilities.

8. Click **Browse** to locate the folder you want to use for the installation. By default, Setup installs VirusScan in this path:

   C:\Program Files\Network Associates\VirusScan NT

9. When you have chosen the component set that you want to install and have specified a destination, click **Next>** to continue.

   - **If you chose a Typical or a Compact component set**, Setup will move directly to the Service Account Usage panel. Read the information given, click **Next>** to continue, then **skip to** Step 10 on page 37.

   - **If you chose a Custom component set**, Setup shows you a wizard panel that lists the components available for installation (Figure 2-6). Select the components you want installed and clear the checkboxes next to those you don't want.

     As you select each component, a description appears near the bottom of the panel. When you have finished your selections, click **Next>**.

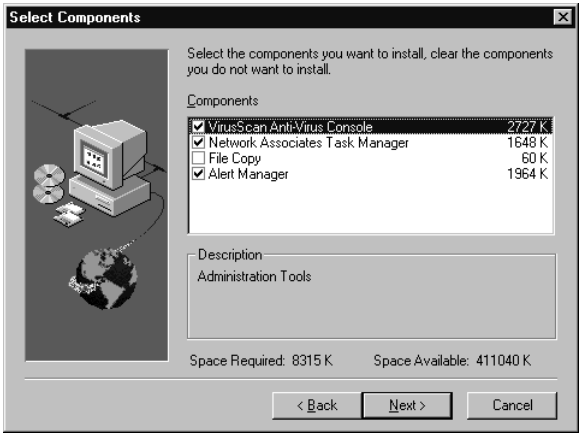


Figure 2-6. Select Components panel

The next three wizard panels ask you to choose which options you want to enable for the Task Manager service, for on-access scanning, and for Alert Manager.

The Task Manager service can add a **Scan for Viruses** menu command that appears whenever you right-click a file or disk on the Windows desktop or from within Windows Explorer. This command conducts an on-demand scan operation on that object immediately, using whatever configuration options you have currently active. Click the checkbox shown to enable this feature.

The on-access scanner can start scan operations as soon as you have finished Setup, and as soon as you start your workstation. Click each checkbox to enable these features.

The Alert Manager service can also start as soon as you finish Setup, and each time you start your workstation. Click each of the checkboxes shown to enable these options.

Click **Next>** at the bottom of each panel to continue. After you've chosen your options, Setup will display the Service Account Usage panel. Read the information given, then click **Next>** to continue.

10. Use the System Account Information panel to choose the type of account you want VirusScan to use to enable its Windows NT services (Figure 2-7).

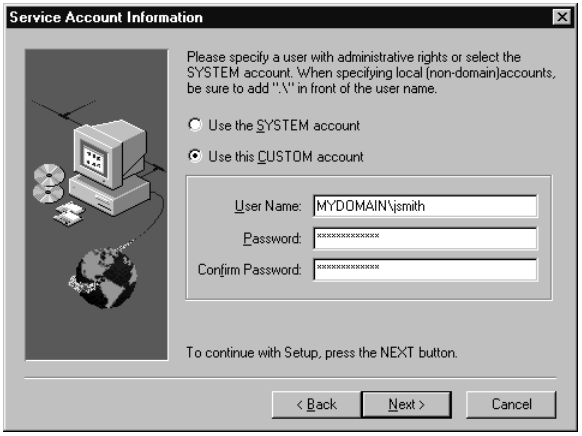


Figure 2-7. Service Account Information panel

11. Your choices are:

- **Use the SYSTEM account.** Select this option only if you cannot or do not want to use a custom account; the default system account does not give VirusScan sufficient system rights to enable some of its functions.

  Alert Manager, for example, will not forward alert messages to Windows NT servers or send them to printers, nor will AutoUpdate retrieve files from Windows NT file shares during scheduled update tasks. Furthermore, VirusScan will not log remote events or perform scheduled scan operations on network drives.

- **Use this CUSTOM account.** Select this option to use a valid account for this workstation with full Administrator rights. This allows VirusScan to enable all of its Windows NT services.

Next, specify the log-in domain, if any, and the user name for the account in the first text box below. Be sure to precede the user name with a backslash (\) whether it follows a domain name or not. Enter the account password, then confirm it, in the following two text boxes.

When you have finished, click **Next>** to continue.

12. In the following panel, Setup will display a default name for the program folder it will create. Type a new program folder name if you wish, or select one of the names listed in the Existing Folders list. To accept the default folder name or the name you've designated, click **Next>**.

    Setup will then summarize all of the options you've chosen in the next panel. If the options shown are correct, click **Next>** to begin copying the VirusScan program files to your hard disk. Otherwise, click **<Back** to return to previous panels to change your choices.

    When it finishes copying files, Setup offers to display the WHATSNEW.TXT file for you to read. Click **Yes** to open the file. This file includes last-minute additions to features, known issues, and other important information. You'll also find a copy of this file in the VirusScan program directory.

13. Click **Finish** to complete your VirusScan installation.

Installing VirusScan on a remote workstation

VirusScan's Setup utility allows you to install the program to any number of other workstations across your network, provided that you have an account with Administrator rights on each target workstation.

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

Installation Steps

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

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

  IMPORTANT: If you suspect that your computer has a virus infection, download the VirusScan installation files onto a computer that is ***not*** infected.

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

If you inserted a CD-ROM disc, you should see a VirusScan welcome image appear automatically.

Follow these steps:

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

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

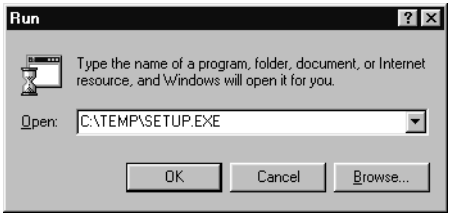


Figure 2-8. Run dialog box

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 VirusScan files. To search for the correct files on your hard disk or CD-ROM disc, click **Browse**.

   NOTE: If your VirusScan copy came on a VirusScan Security Suite or a Total Virus Defense CD-ROM disc, you must also specify which folder contains VirusScan for Windows NT. To learn where to find the correct folder, see the CONTENTS.TXT file included with either CD-ROM disc.

   Setup will start and display its welcome panel (see Figure 2-9 on page 40).

Figure 2-9. Welcome to Setup wizard panel

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

   The next wizard panel displays the VirusScan end-user license agreement. Read this agreement carefully—if you install VirusScan, 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.

5. Setup asks you whether you want to install VirusScan on your local workstation or on other computers elsewhere on your network (see Figure 2-3 on page 34). Click **Remote Installation**, then click **Next>**.

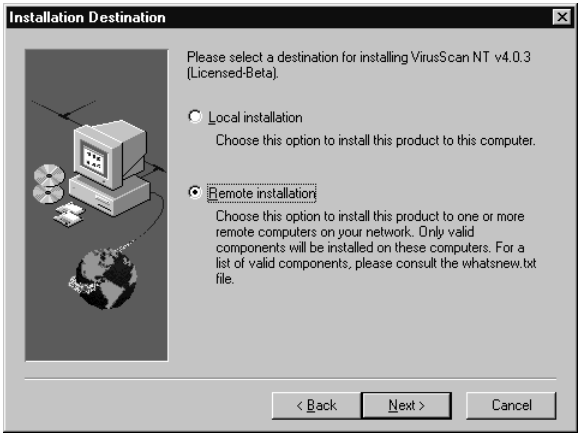


Figure 2-10. Installation Destination panel

The Select Remote Server panel appears (Figure 2-11). Here, you can specify which computers you want to install VirusScan on.

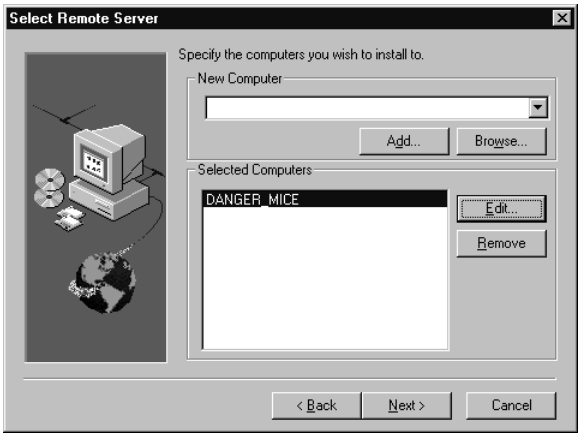


Figure 2-11. Select Remote Server panel

Follow these steps:

a. Click **Browse** to open a dialog box where you can locate a computer on the network (Figure 2-12).

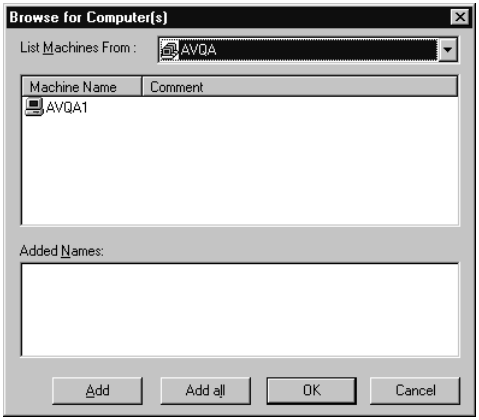


Figure 2-12. Browse for Computers dialog box

b. Choose the domain you want to search from the **List Machines From** menu. Setup will connect to the network and display all accessible computers in that domain.

c. Select one or more computers from the list shown. To select more than one name, press the CTRL key on your keyboard as you click each name. To select a continuous range of names, click the first name in the range, then press the SHIFT key on your keyboard as you click the last name in the range.

d. Click **Add** to select the computers you chose. The names will appear in the list at the bottom of the dialog box. To add all computers in the entire domain, click **Add All**. Next, click **OK** to close the dialog box and return to the Select Remote Server panel.

6. The computers you designated now appear in the New Computer text box. Click **Add** to open a dialog box where you can specify the user name and password for an account with Administrator rights on the target workstation (Figure 2-13).

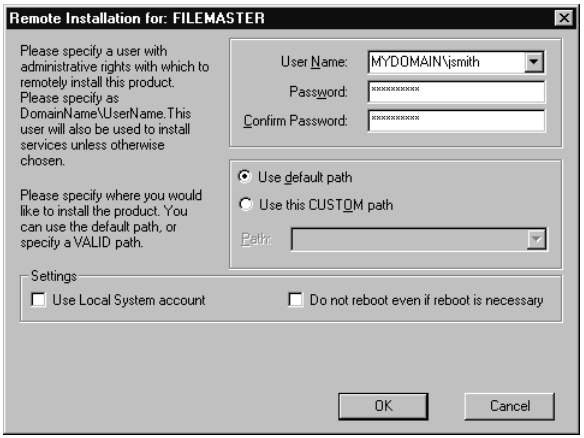


Figure 2-13. Remote Installation dialog box

7. Enter a user name in the text box provided, or choose any of the accounts listed. Be sure to precede the user name with a domain name and a backslash (\). Next, enter a password, then confirm it, in the following two text boxes.

8. In the center of the dialog box, specify where on the target workstation you want to install the VirusScan program files. You can choose to install VirusScan in its default path, which is

   C:\Program Files\Network Associates\VirusScan NT

   or you can designate a different path for this workstation. Be sure that the path you want to use actually exists on the target workstation—Setup will not create it.

9. Select the **Use Local System Account** checkbox to tell VirusScan to enable its Windows NT services through the default system account on the target workstation. If you do not select this checkbox, VirusScan will use the account you specified at the top of the dialog box.

   Select the system account option only if you cannot or do not want to use a custom account for this workstation. The default system account does not give VirusScan sufficient system rights to enable some of its functions. Alert Manager, for example, will not forward alert messages to Windows NT servers or send them to printers, nor will AutoUpdate retrieve files from Windows NT file shares during scheduled update tasks. Furthermore, VirusScan will not log remote events or perform scheduled scan operations on network drives.

10. Select the **Do not reboot even if reboot is necessary** checkbox to prevent the target workstation from restarting after the installation. Some VirusScan services require you to reboot the workstation before they activate. Those services will remain inactive until you restart that workstation.

11. Click **OK** to close the dialog box. Setup will list the servers you've designated for installation in the Confirm Installation Settings panel. If these settings are correct, click **Next>** to start copying files to the target workstations. Otherwise, click **<Back** to change your choices.

    Setup will install VirusScan on each target workstation silently. Workstation users will see only a minimized program button in the Windows taskbar during the installation.

NOTE: If users working on the target computer click the minimized silent installation button in the taskbar, they will see a small dialog box that describes the status of the installation. If they click **OK** to close the dialog box, the window will minimize itself again. If, however, they click the closebox, the installation will stop immediately.

Performing a "silent" installation

If you manage a network and want to deploy VirusScan as your standard anti-virus security application, you can use the Setup utility's "silent" installation feature to set up VirusScan on each network node with little or no interaction from end users. During a silent installation, Setup does not display any of its usual wizard panels or windows, or offer the end user any configuration options. Instead, you preset these choices and run Setup in the background on each target workstation. If you wish, you can even install VirusScan on any unattended workstations or without the end user's knowledge, provided you have all the necessary administrative privileges.

A silent installation consists of two major steps. First, you must install the same VirusScan components on your administrative computer or server that you want Setup to install on each target workstation. A special Setup mode records the choices you make during installation and preserves them in a configuration file called SETUP.ISS. Next, you must use a different Setup mode to install an identical VirusScan configuration on each target system. Setup will use the SETUP.ISS file you create in the first step to guide each subsequent installation you perform.

Recording your preferences

To record your installation preferences, follow these steps:

1. Look for an existing SETUP.ISS file inside the \WINDOWS folder on your administrative computer. If you find a file with that name in the WINDOWS folder, rename it or delete it.

   As you record your installation preferences, Setup will save them into a new SETUP.ISS file in the same location.

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

   The Run dialog box will appear (Figure 2-14).

Figure 2-14. Run dialog box

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

   Here, <X> represents the drive letter for your CD-ROM drive or the path to the folder that contains your extracted VirusScan files. The `-R` tells Setup to run in its "record" mode.

   NOTE: If your VirusScan copy came on a VirusScan Security Suite or a Total Virus Defense CD-ROM disc, you must also specify which folder contains VirusScan for Windows NT. To learn where to find the correct folder, see the CONTENTS.TXT file included with either CD-ROM disc.

   To search for SETUP.EXE on your hard disk or CD-ROM disc, click **Browse**. Be sure to add `-R` to the run statement if you use this option.

4. Follow the installation steps outlined on pages 32 to 38 to choose the components and the settings you want each of the target workstations to have.

   Setup notes the choices you make at each step and records them as entries in SETUP.ISS.

   IMPORTANT: Take particular care during this initial installation to respond to any questions that appear in the wizard panels and to follow the installation steps in the sequence presented, or the silent installation you run later will abort. You may not backtrack during the installation to change your settings.

   To specify different options, you will need to begin the installation again in order for Setup to record your choices correctly. If you plan to install VirusScan on unattended workstations, be sure to specify options that do not require user interaction.

   The installation will also abort if VirusScan detects a virus on your computer.

5. Once you've completed the installation, click **Finish** to quit Setup.

Editing the SETUP.ISS file to specify an installation directory

If you want Setup to install VirusScan in a particular directory, you will need to edit the SETUP.ISS file you created when you installed VirusScan on your administrative computer. To make network administration easier, for example, you might want to install all of your VirusScan copies in the same directory on each network node.

SETUP.ISS is simply a specially formatted text file similar to configuration files such as WIN.INI or SYSTEM.INI. You can open it in any text editor and change any of its entries to suit your needs.

NOTE: Network Associates recommends that you make only limited changes to the SETUP.ISS file. If you want complete control over the installation process, or if you want to specify the configuration options for each copy of VirusScan in advance, you can use ISeamless, a powerful Network Associates scripting tool designed for this purpose. Contact Network Associates Technical support for details.

SETUP.ISS specifies an installation directory as a value for the variable **szDir,** which you'll find listed beneath the header **[SdSetupType-0]**. By default, this entry reads:

```
[SdSetupType-0]
szDir=C:\Program Files\Network Associates\VirusScan NT\
Result=401
```

To specify a different installation directory, replace the path shown with the path you want. The installation directory you specify here will override the default installation directory on each target system.

IMPORTANT: Setup creates a unique SETUP.ISS file for each Network Associates product on each platform. You must use the file that corresponds to the operating system running on the target workstation. You may not, for example, use a SETUP.ISS file created during a VirusScan for Windows 95 installation to control a VirusScan for Windows NT installation.

6. Save the file in text format, then quit your text editor.

IMPORTANT: Network Associates recommends that you use the SETUP.ISS file you created to perform a test installation on a single workstation before you use it to deploy VirusScan across your network.

Running a silent installation

Once you have a SETUP.ISS file that lists all of the components and settings you want each workstation on your network to have, you can replicate these settings exactly for every VirusScan copy you install. See "Recording your preferences" on page 44 to learn how to create the SETUP.ISS file.

You can run a silent installation in a variety of ways, and with different levels of interaction with network users. You can, for example, create a script for your users that runs a silent VirusScan installation as soon as they connect to an authentication server, with no further interaction beyond that needed to log in. You can also ask your users to run the installation from a designated server. Still other options include deploying VirusScan through a network management application such as Zero Administration Client (ZAC) or Management Edition from Network Associates, System Management Server (SMS) from Microsoft, or similar packages.

Whichever method you choose, you must first prepare the VirusScan package for installation, then run Setup in its silent mode.

Follow these steps:

1. Copy the VirusScan installation files from the VirusScan CD-ROM disc or the folder on your administrative computer in which your store them to a VirusScan directory on a central server. Your users or your network management application will install VirusScan from this server.

2. Locate the SETUP.ISS file stored in the VirusScan directory on the central server. Rename or delete this file.

3. Copy the SETUP.ISS file you created when you ran the recorded installation on your administrative computer to the VirusScan directory on the central server. You'll find the file you need to copy in the WINDOWS directory on your administrative computer. See "Recording your preferences" on page 44 to learn how to record your installation.

   Once you finish this step, your users or your network management application can run Setup in its silent mode to replicate the installation you recorded.

To run Setup in silent mode, include the line `<X>:\SETUP.EXE -S` in any login script you write or any instructions to your users that describe how to run Setup. In this line, `<X>` represents the path to the folder on the server that contains the VirusScan installation files and the SETUP.ISS file you created. The `-S` tells Setup to run in silent mode. By default, Setup restarts the workstation when it has finished installing files.

If you do not want Setup to reboot each target workstation, you must edit the SETUP.ISS file you created during your recorded installation. Here, you would change the value in the **BootOption** entry beneath the heading **[sdFinishReboot - 0]** from its current value to zero (0). This tells Setup not to force the target workstation to reboot.

As a further step toward enforcing a consistent anti-virus security policy across your network, you can also copy a configuration file with the options you want your users to have into the installation directory on each workstation. To learn how to save your settings in a configuration file, see "Using VirusScan menus" on page 125.

NOTE: To preset your configuration options so that VirusScan installs with them already in place, use the Network Associates ISeamless scripting utility. This utility gives you complete control over installation and configuration options. Contact your sales representative or Network Associates technical support for details.

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, or from the possibility that the files you downloaded have become corrupted, 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 VirusScan package.

To validate your files, follow these steps:

1. Install VirusScan as described in "Installation Steps" on pages 32 to 38.
2. Click **Start** in the Windows taskbar, point to **Programs**, then choose **Command Prompt**.
3. In the window that appears, change your command-line prompt to point to the directory that contains the VirusScan files you installed. If you chose the default installation options, you'll find the files in this path:

   C:\Program Files\Network Associates\VirusScan NT

   If you installed VirusScan 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 VirusScan 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 *.* >prn` 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 VirusScan, you need to compare the validation codes against the packing list supplied with the program. 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 VirusScan 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 >prn` 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 executable file name—that is, those with .EXE and .DLL extensions —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 VirusScan 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 VirusScan to learn the license terms that cover your use of the program.

Validation codes for some files, including those with .INI and .VSC extensions, *might not match* those shown in PACKING.LST, as Setup can make changes to these files during installation.

Testing Your Installation

Once you install it, VirusScan 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 the European Institute of Computer Anti-virus Research (EICAR), a coalition of anti-virus vendors, as a method for their customers to test any anti-virus software installation.

To test your installation, follow these steps:

1. Open a standard Windows text editor, such as Notepad, then type:

```
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 VirusScan and allow it to scan the directory that contains EICAR.COM. When VirusScan 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.

Getting Started 3

Enabling VirusScan components

VirusScan for Windows NT consists of an AntiVirus Console application and a set of Windows NT services that provide the program's scanning, response and reporting functions. You can use the AntiVirus Console to configure scan tasks, set on-access scan operations and choose other program options. The Console also allows you to see scanning statistics and receive virus alert messages.

Although you need the AntiVirus Console to configure the program services, you do not need to keep it running in order for VirusScan to perform its background scanning operations or any scan tasks you schedule. You must, however, keep the Network Associates Task Manager service and the Network Associates McShield service running to perform these functions.

NOTE: You do *not* need to start the VirusScan Windows NT services separately, although you can enable and disable them from the Windows NT Services control panel.

Because VirusScan cannot always get the information it needs to determine the status of these services, however, controlling VirusScan functions through the control panel can cause unpredictable program behavior, particularly for VirusScan's on-access component. Network Associates recommends that you use the AntiVirus Console to control program operations instead.

Starting the VirusScan AntiVirus Console

To start the AntiVirus Console

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

  The VirusScan Console window appears (see Figure 3-1 on page 52).

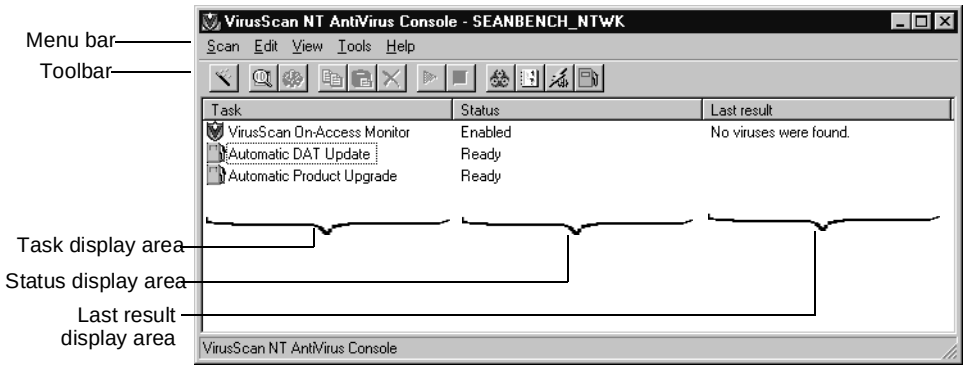


Figure 3-1. VirusScan Console window

The Console window includes a menu, a toolbar, a task list area, and a status bar, each of which gives you necessary information or the ability to create, configure, edit, or delete all VirusScan scan operations and other tasks. The following sections describe each element in more detail.

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. VirusScan can perform three types of tasks: on-access tasks; on-demand or scheduled tasks; and an Automatic DAT Update or Automatic Product Upgrade task. The task list initially displays a default set of tasks for updating virus definition files and upgrading program files. The list also includes the VirusScan On-Access Monitor, a utility for configuring and monitoring VirusScan's on-access scanning component. The task list does not include any on-demand or scheduled tasks by default—you can create these tasks to suit your needs.

The VirusScan On-Access Monitor

VirusScan's on-access scanner looks for viruses in files that you open, save, or copy to and from your workstation. You can use the On-Access Task Monitor to specify which files the scanner examines and how VirusScan 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 start a scan operation immediately. You can specify which volumes on your workstation you want to scan, tell VirusScan how to respond if it finds an infected file, and choose options for alerting and logging, then have the program go to work. Scheduled tasks run at specific times, or repeatedly at specific intervals, and can include all of the options you might specify for an on-demand scan operation. VirusScan does not come with any pre-configured on-demand or scheduled tasks. To learn how to configure on-demand tasks, or how to schedule scan tasks, see Chapter 5, “On-demand and Scheduled Scanning.”

Automatic DAT Update and Automatic Product Upgrade tasks

AutoUpdate automatically retrieves new virus definition files for use with VirusScan, while AutoUpgrade retrieves new program files for VirusScan itself. from an FTP site or 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. AutoUpgrade automatically retrieves new program files that update VirusScan itself. To learn how to create and schedule AutoUpdate tasks, see Chapter 7, “Updating NetShield.”

Task statistics

To see the most recent status information and results from any listed on-access or on-demand scan task, select it, then choose **Statistics** from the **Scan** menu to open the Task Statistics dialog box (Figure 3-2). You can also double-click any listed task to display this dialog box. The Automatic DAT Update and Automatic Product Upgrade tasks do not display task statistics this way—double-clicking either task will display its property page.

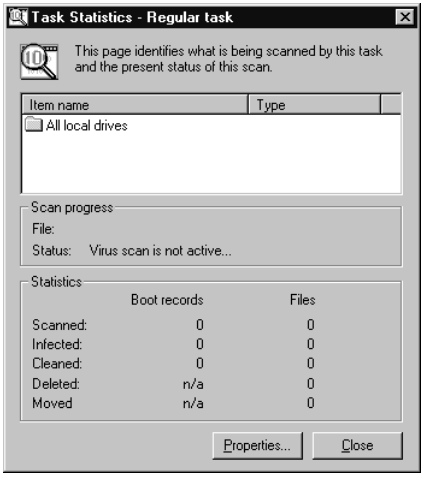


Figure 3-2. Task Statistics window

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 summarizes latest results for a listed task.

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 Console 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.

Table 3-1 lists the toolbar buttons in the order in which they appear on the AntiVirus console. The table also shows the equivalent menu command for each button and describes what the command does. Table 3-2 on page 58 provides this same information, sorted by how the commands appear in the Console's menus.

Table 3-1. AntiVirus Console command overview - by toolbar button

Toolbar Button	Menu Equivalent	Description
		Click this button in the Console toolbar or choose **Scan Wizard** from the **Scan** menu to start the Scan Wizard. The first Scan Wizard panel will appear. Follow the instructions shown on each panel to schedule a scan operation or configure an on-demand scan task.

Table 3-1. AntiVirus Console command overview - by toolbar button

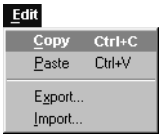
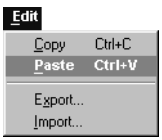
Toolbar Button	Menu Equivalent	Description
		Click this button in the Console toolbar, or choose **New Task** from the **Scan** menu to create a new task. A Task Properties dialog box will appear. See Chapter 6, "Scheduling and Running On-Demand Scan Operations," to learn how to configure your new task.
		Select a task listed in the Console window, then click this button or choose **Properties** from the **Scan** menu to open the Task Properties dialog box for that task. See Chapter 6, "Scheduling and Running On-Demand Scan Operations," to learn how to change your task configuration.
		Select a task listed in the Console window, then click this button or choose **Copy** from the **Scan** menu to copy the task to the Windows clipboard. Use this feature to copy the task settings for an on-demand task to use as a template for other, similar tasks.
		Click this button or choose **Paste** from the **Scan** menu to paste a task you've copied to the Windows clipboard back into the task list area in the Console window. When you paste the task into the Console window, VirusScan prompts you to rename it. Type a name, then press **ENTER**. The Task Properties dialog box opens, so that you can modify the task before you save it. See "Creating an on-demand task in the AntiVirus Console" on page 90 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.

Table 3-1. AntiVirus Console command overview - by toolbar button

Toolbar Button	Menu Equivalent	Description
		Select a task listed in the Console window, then click this button, or choose **Delete** from the **Scan** menu, to remove the task from the Console window. VirusScan 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. You can delete only tasks that you create. You may not delete the On-Access Monitor, the Automatic DAT Update, or the Automatic Product Upgrade that come with the Console. You can, however, *disable* any task that you do not want to run.
		Select a task listed in the Console window, then click this button or choose **Start** from the **Scan** menu to start that task. The task will start immediately and run with the options you've already given it. To start the on-access scanner, select the On-Access Task Monitor in the list, then Choose **Enable** from the **Scan** menu. Note that the **Start** command in the **Scan** menu has changed to **Enable**. 
		Select an active task listed in the Console window, then click this button or choose **Stop** from the **Scan** menu to stop that task. To stop the on-access scanner, select the On-Access Task Monitor in the list, then Choose **Disable** from the **Scan** menu. Note that the **Stop** command in the **Scan** menu has changed to **Disable.** 

Table 3-1. AntiVirus Console command overview - by toolbar button

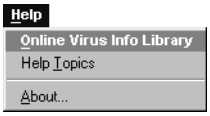
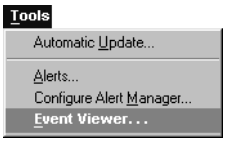
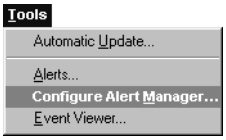
Toolbar Button	Menu Equivalent	Description
		Click this button or choose **Online Virus Info Library** from the **Help** menu to connect to the Virus Information Library. VirusScan starts your default web browser software and connects to the Network Associates website to display the library.
		Click this button or choose **Event Viewer** from the **Tools** menu to open the Windows NT Event Viewer. The Event Viewer allows you to monitor the state of your workstation, including the state of VirusScan's Windows NT Services. You can also click the **Start** button, point to **Programs**, point to **Administrative Tools (Common)**, then choose **Event Viewer** to see the same dialog box.
		Click this button or choose **Configure Alert Manager** from the **Tools** menu to open the Alert Manager Properties dialog box. See Chapter 7, "Sending Alert Messages," to learn how to tell VirusScan to alert you when it finds a virus.
		Click this button or choose **Automatic Update** from the **Tools** menu to open the Automatic Update / Upgrade Properties dialog box. See Chapter 8, "Updating and Upgrading VirusScan," to learn how to configure Automatic DAT Updates and Automatic Product Upgrades.

Table 3-2 lists the menu items in the order in which they appear in the AntiVirus console. The table also shows the equivalent toolbar buttons, if any exist, for each menu item and describes what the command does. Table 3-1 on page 54 provides this same information, sorted by the order in which the buttons appear in the Console toolbar.

Table 3-2. AntiVirus Console command overview - by menu item

Menu	Toolbar Equivalent	Description
		Choose **New Task** from the **Scan** menu, or click this button in the Console toolbar, to create a new task. A Task Properties dialog box will appear. See Chapter 6, "Scheduling and Running On-Demand Scan Operations," to learn how to configure your new task.
		Choose **Scan Wizard** from the **Scan** menu or click this button in the Console toolbar to start the Scan Wizard. The first Scan Wizard panel will appear. Follow the instructions shown on each panel to schedule a scan operation or configure an on-demand scan task.
		To stop the on-access scanner, select the On-Access Task Monitor in the list, then Choose **Disable** from the **Scan** menu, or click the toolbar button shown.  To stop an active on-demand task, select the task in the Console window, then choose **Stop** from the **Scan** menu, or click this same toolbar button. Note that the **Disable** command in the **Scan** menu changes to **Stop** when you select an active on-demand task.

Table 3-2. AntiVirus Console command overview - by menu item

Menu	Toolbar Equivalent	Description
		To start the on-access scanner, select the On-Access Task Monitor in the list, then Choose **Enable** from the **Scan** menu, or click the toolbar button shown. The task will run with the options you've chosen for it. To start an on-demand task with the options you've set for it, select the task in the Console window, then choose **Start** from the **Scan** menu, or click this same toolbar button. Note that the **Enable** command in the **Scan** menu changes to **Start** when you select an on-demand task. 
	None	Select an on-demand task you've created, then choose **Rename** from the **Scan** menu to highlight the task in the Console window. Next, type the new task name, then press ENTER. Note that you cannot rename the VirusScan On-Access Monitor, the Automatic DAT Update task, or the Automatic Product Upgrade task.

Table 3-2. AntiVirus Console command overview - by menu item

Menu	Toolbar Equivalent	Description
		Select a task listed in the Console window, then choose **Delete** from the **Scan** menu, or click this button, to remove the task from the Console window. VirusScan 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. You can delete only tasks that you create. You may not delete the On-Access Monitor, the Automatic DAT Update, or the Automatic Product Upgrade that come with the Console. You can, however, *disable* any task that you do not want to run.
	None	Select a task listed in the Console window, then choose **Statistics** from the **Scan** menu, or simply double-click the task, to displays the status and results of the last scan operation. If you select an active task, VirusScan updates the status and results dynamically, as the scan proceeds. Note that you cannot display statistics for either the Automatic DAT Update or the Automatic Product Upgrade tasks with these methods.
	None	Choose **Activity Log** from the **Scan** menu to open the log file that VirusScan uses to record its actions during scan operations. See "Choosing Reports options" on page 97 to learn more about creating log files.

Table 3-2. AntiVirus Console command overview - by menu item

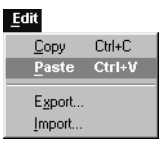
Menu	Toolbar Equivalent	Description
		Select a task in the Console window, then choose **Properties** from the **Scan** menu, or click this button, to open the Task Properties dialog box for that task. See Chapter 6, "Scheduling and Running On-Demand Scan Operations," to learn how to change your task configuration.
	None	Choose **Exit** from the **Scan** menu to close the AntiVirus Console. Note that closing the AntiVirus Console does not stop any active on-access or on-demand tasks. Nor do you need to keep the Console window open to run scheduled scan operations.
		Select a task listed in the Console window, then choose **Copy** from the **Edit** menu, or click this button, to copy the task to the Windows clipboard. Use this feature to copy the task settings for an on-demand task to use as a template for other, similar tasks.
		Choose **Paste** from the **Edit** menu, or click this button, to paste a task you've copied to the Windows clipboard back into the task list area in the Console window. When you paste the task into the Console window, VirusScan prompts you to rename it. Type a name, then press **ENTER**. The Task Properties dialog box opens, so that you can modify the task before you save it. See "Creating an on-demand task in the AntiVirus Console" on page 90 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.

Table 3-2. AntiVirus Console command overview - by menu item

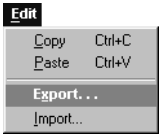
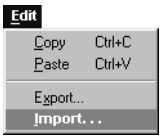
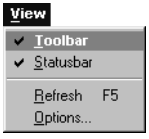
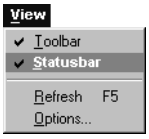
Menu	Toolbar Equivalent	Description
	None	.Select a task that you created from the list in the Console window, then choose **Export** from the **Edit** menu. Name your file in the Select Export File dialog box that appears and choose a location to save it, then click **Save**. VirusScan saves the task as a .VSC file that records all of the task options you chose. You can copy this file to another workstation, mail it, or otherwise distribute it for use with any other VirusScan installation.
	None	Choose **Import** from the **Edit** menu, then locate a file with the extension .VSC in the Select Import File dialog box that appears. Next, click **OK** to have it appear in the Console window. VirusScan will prompt you to name the task. Type a name, then press ENTER. VirusScan will open the Task Properties dialog box to give you an opportunity to modify the task before you save it. See Chapter 6, "Scheduling and Running On-Demand Scan Operations," to learn how to change task settings. Click **OK** to close the Task Properties dialog box when you have changed the task settings.
	None	Choose **Toolbar** from the **View** menu to hide or display the Console's toolbar buttons. A check mark beside the item indicates that the toolbar is active. When the toolbar is hidden, no checkmark appears.
	None	Choose **Statusbar** from the **View** menu to hide or display the status bar at the bottom of the Console window. A check mark beside the item indicates that the status bar is active. When the status bar is hidden, no checkmark appears.

Table 3-2. AntiVirus Console command overview - by menu item

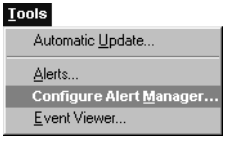
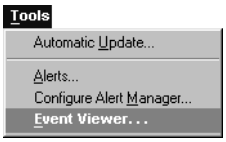
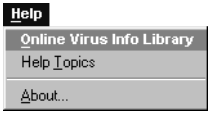
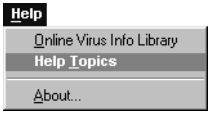
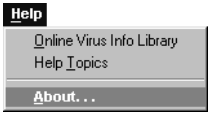
Menu	Toolbar Equivalent	Description
	None	Choose **Refresh** from the **View** menu to update the task list display immediately.
	None	Choose **Options** from the **View** menu to open a dialog box where you can tell VirusScan how often to automatically refresh the task list display. By default, the 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.
		Choose **Automatic Update** from the **Tools** menu, or click this button, to open the Automatic Update / Upgrade Properties dialog box. See Chapter 8, "Updating and Upgrading VirusScan," to learn how to configure Automatic DAT Updates and Automatic Product Upgrades.
	None	Choose **Alerts** from the **Tools** menu to open the Alert Properties dialog box. From there you can activate the Alert Manager and edit the priority and content of any alert messages VirusScan sends. See Chapter 7, "Sending Alert Messages," to learn how to configure and send alert messages.
		Choose **Configure Alert Manager** from the **Tools** menu, or click this button, to open the Alert Manager Properties dialog box. See Chapter 7, "Sending Alert Messages," to learn how to tell VirusScan to alert you when it finds a virus.

Table 3-2. AntiVirus Console command overview - by menu item

Menu	Toolbar Equivalent	Description
		Choose **Event Viewer** from the **Tools** menu, or click this button, to open the Windows NT Event Viewer. The Event Viewer allows you to monitor the state of your workstation, including the state of VirusScan's Windows NT Services. You can also click the **Start** button, point to **Programs**, point to **Administrative Tools (Common)**, then choose **Event Viewer** to see the same dialog box.
		Choose **Online Virus Info Library** from the **Help** menu, or click this button, to connect to the Virus Information Library. VirusScan starts your default web browser software and connects to the Network Associates website to display the library.
	None	Choose **Help Topics** from the **Help** menu to open VirusScan's online help file.
	None	Choose **About** from the **Help** menu to see copyright information, serial numbers, virus definition file version numbers, and other information about your copy of VirusScan.

Using VirusScan's system tray icon

VirusScan's on-access scanner installs and activates itself by default when you do a Typical setup. Once active, the scanner displays a shield icon in the Windows NT system tray.

Double-clicking the icon will display status information and results from the most recent on-access scan operation (Figure 3-3). The Statistics dialog box displays the total number of files the scanner examined, how many of them it found viruses in, and the number of different response actions it took.

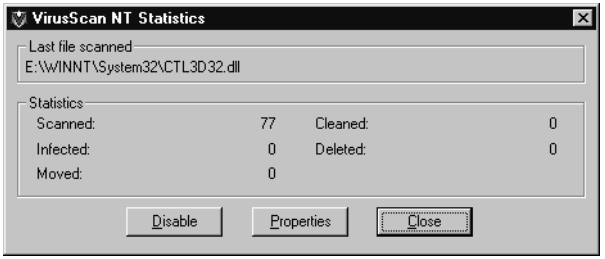


Figure 3-3. VirusScan NT Statistics dialog box

From here, you can click **Disable** to stop the Network Associates McShield service, which does VirusScan's on-access scanning. The system tray icon and the icon beside the VirusScan On-Access Monitor in the Console window will change to , which indicates that the service is not active. To reactivate the service, click **Enable** in the Statistics dialog box.

Clicking **Properties** will open the VirusScan Properties dialog box, where you can configure the on-access scanner. Click **Close** to dismiss the dialog box.

The system tray icon also hides a shortcut menu that gives you access to these same functions, along with some others. To display the shortcut menu, right-click the icon, then choose the command you want. Choose from:

- **Statistics.** Choose this to open the Statistics dialog box (Figure 3-3).
- **Disable.** Choose this to deactivate the on-access scanner. To reactivate the scanner, choose **Enable** from this same menu.
- **Properties.** Choose this to open the VirusScan Properties dialog box.
- **Console.** Choose this to display the AntiVirus Console window.
- **Alerts.** Choose this to open the Alert Manager Properties dialog box.
- **About.** Choose this to see copyright information, serial numbers, virus definition file version numbers, and other information about your copy of VirusScan.

Creating a task with the Scan wizard

VirusScan comes with a preconfigured Windows NT service 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 VirusScan 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 traffic on your workstation for viruses. You can use VirusScan'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 VirusScan and your network's susceptibility to viruses.

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

1. Start the AntiVirus Console. See "Starting the VirusScan AntiVirus Console" on page 51 for details.
2. Choose **Scan Wizard** from the **Scan** menu, or click  in the Console toolbar.

   The first Scan wizard panel appears (Figure 3-4).

Figure 3-4. Welcome to Scan Wizard panel

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

   The Scan wizard displays a panel where you can specify which volumes you want VirusScan to examine for viruses (see Figure 3-5 on page 67). By default, VirusScan looks at all local hard disk volumes on your workstation, 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 3-5. 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 3-6).

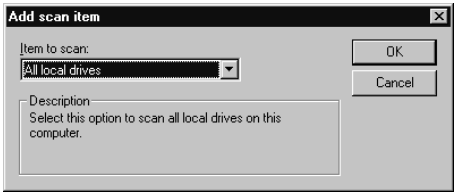


Figure 3-6. Add Scan Item dialog box

   Next, choose a scan target from the list. You can choose to scan all local drives, a particular drive or folder, or a particular file. If you choose to scan a drive, folder, or file, enter the path to the target object 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, folder, or drive. When you have finished, click **OK** to close the dialog box.

   - **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 3-7).

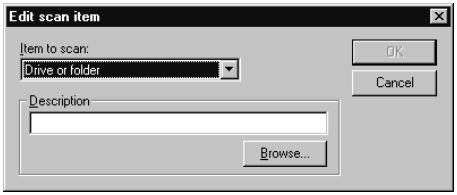


Figure 3-7. Edit Scan Item dialog box

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 VirusScan to perform your scan operation (Figure 3-8).

Figure 3-8. Choose scan options panel

6. Choose your scan options. You can

   - **Scan volume subfolders.** By default, VirusScan 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, VirusScan's on-demand scanner examines files compressed with these formats: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, and .ZIP. To prevent VirusScan from scanning these files, clear the **Scan inside compressed files** checkbox.
   - **Skip boot record scanning.** VirusScan ordinarily will scan your master boot record and the boot blocks on your hard disk for boot-sector viruses. Although the majority of new viruses are macro viruses, boot sector viruses continue to spread and can cause your system harm. Network Associates recommends that you scan your boot record regularly, but if doing so will interfere with system operations, select this checkbox to bypass this type of scan operation.
   - **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** button. To see or designate those file name extensions, click **File Types** to open the Program File Extensions dialog box (see Figure 3-9 on page 69).

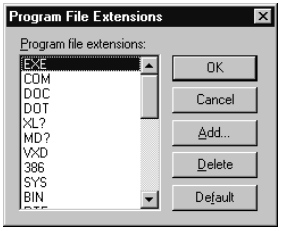


Figure 3-9. Program File Extensions dialog box

By default, VirusScan scans files with the extensions .EXE, .COM, .DOC, .DOT, .XL?, .MD?, .VXD, .386, .SYS, .BIN, .RTF, .OBD, .DLL, .SCR, .OBT, .PP? .POT, .OLE, .SHS, .MPP, .MPT, .XTP, .XLB, .CMD, .OVL, and .DEV. This list covers nearly all potentially susceptible files, including all Microsoft Office file types, which are susceptible to macro viruses. The ? character is a wildcard that enables VirusScan to examine files similar in type, such as document and template files.

- To add to the list, click **Add**, then type the extension you want VirusScan 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 workstation, 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 (Figure 3-10).

Figure 3-10. Choose alert and logging options panel

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

   - **Send alerts via Alert Manager.** To have VirusScan 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 VirusScan 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 VirusScan can use to record its actions. By default, the program uses a file called SCAN ACTIVITY LOG.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. VirusScan 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 tell VirusScan how to respond when it detects a virus (Figure 3-11).

Figure 3-11. Specify virus response panel

10. Choose one of the listed responses. You can:

    - **Continue Scanning.** This tells VirusScan to note when it detects a virus, then to continue scanning without taking any other action. If you have configured alert and logging options, VirusScan 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 VirusScan to quarantine the infected file in a specific folder. By default, VirusScan stores the file in a folder named Infected within its program directory. To specify a different location, enter the path in the text box provided, or click **Browse** to locate a suitable folder.
    - **Clean infected file.** This tells VirusScan to try to remove the virus from the infected file and restore it to its original, uninfected condition. The data files that come with VirusScan include virus removers for most virus types, but in some cases, VirusScan 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 VirusScan 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 VirusScan run your new task immediately, or save it to run or schedule for later (Figure 3-12).

Figure 3-12. Run or save task panel

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

    - **Run task now without saving.** This tells VirusScan to run the task once, then discard it.
    - **Save task without running.** This tells VirusScan 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 VirusScan 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 VirusScan to run your task immediately, you'll see the New Scan Task dialog box appear as the program begins scanning the volumes you specified (Figure 3-13). You can minimize this window to conduct your scan operation in the background.

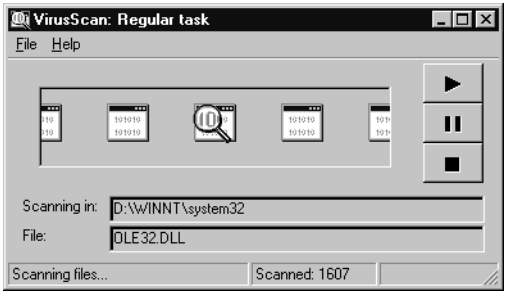


Figure 3-13. New Scan task window

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

Removing Infections From Your System 4

If you suspect you have a virus...

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

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

The safest course of action you can take is to install VirusScan and perform an immediate and thorough system scan.

As it installs itself, VirusScan will examine your computer's memory and your hard disk's boot sectors to verify that it can safely copy its files to your hard disk without risking their infection. If VirusScan detects a virus during Setup, it will alert you to its presence, log the incident in its activity log, and deny access to the file. You should consider conducting a thorough, on-demand system scan as soon as possible after installation, then clean, move, or delete any infected files you find. See "Responding to viruses or malicious software" on page 75 for details.

Alternatively, you could try to remove the virus from the file yourself. Network Associates does not recommend this method because of the potential for file corruption, but the online Virus Information Library stored on the Network Associates website has information that can help you remove a virus from an infected file. To see this information, start your preferred web browser application, then enter the following web address:

http://vil.mcafee.com/vil/<document number>.asp

In the address listed, <document number> represents a technical document in the Virus Information Library. Replace <document number> with one of these numbers:

0118 0319 0322 0323 0327 1145

NOTE: Document numbers might change. See the online Virus Information Library table of contents for current information.

Creating an emergency disk

Although VirusScan's program modules can usually detect and remove a virus before it poses a threat to your system, in some circumstances you should start your workstation from a floppy disk and conduct a system scan in order to remove viruses lurking in memory or concealed in the boot sectors on your hard disk. If you have a virus present on your system during Setup, for example, you could risk infecting some of VirusScan's program files.

To create an Emergency Disk, follow these steps:

1. Click **Start**, point to **Programs**, then choose **Command Prompt** to open a Command Prompt window.
2. Change directories to the \EDU directory within the VirusScan program directory. If you have installed VirusScan to its default program directory, you can type this line at the command prompt:

   ```
   cd \program files\network associates\virusscan nt\edu
   ```

3. Insert a blank, *formatted* 1.44MB disk into your floppy drive.
4. Type this line at the command prompt:

   ```
   naidskim /wa /t144 /f<x>:\progra~1\networ~1\viruss~1
   \edu\edisk.img
   ```

   Be sure to substitute the letter of the drive on which you have VirusScan installed for the <x> in the line shown. If you installed the program to a different directory, substitute the correct directory path for that shown, also.

   The emergency disk utility will run a batch file that copies Emergency Disk files from a disk image to your floppy drive. The options shown tell the batch file to write to your A: drive, to a 1.44 MB floppy disk, and to take files from the EDISK.IMG file stored in the \EDU directory. To copy the files to a different drive, or from a different path, substitute the correct values for those shown. To learn about the correct syntax for the copy utility, type `naidskim` at the command line without any options.

5. When the utility finishes creating the Emergency Disk, label the disk, lock it, then store it in a safe place.

Responding to viruses or malicious software

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

Responding when the on-access scanner detects a virus

By default, VirusScan's on-access scanner looks for viruses each time you run, copy, create, or rename any file on your local system, whenever you read from a floppy disk, or whenever you leave a disk in the drive as you shut your workstation down.

When you first install it, the scanner automatically tries to clean any infected file it finds during a scan operation. If it cannot clean the file, it appends a .VIR extension to it and denies access to it. To learn how to configure the scanner so that it responds in other ways, see Chapter 5, "Using the On-Access Scanner."

The scanner will also notify you through Alert Manager. By default, Alert Manager sends out only a Windows NT network alert message, which shows up only on your local workstation (Figure 4-1).

Figure 4-1. Network alert message

Here, VirusScan has detected the EICAR test "virus," a non-infectious, non-replicating text file used specifically to test anti-virus software. Click **OK** to dismiss the network message.

Unless VirusScan does not have a cleaner for the virus, as in the example shown, you do not need to take any further action. VirusScan will also record the incident in its activity log, where you can review the results of its scan operations at your convenience.

If no cleaner exists, you can delete the file and restore it from an uninfected backup file, isolate it in a quarantine folder, or send it to Network Associates for analysis. To learn how to choose other response options, see Chapter 5. To learn how to send sample files to Network Associates, see "Reporting new items for anti-virus data file updates" on page xix.

Responding when VirusScan detects a virus

When you first install VirusScan and start an on-demand scan operation, the program will look at all files on your C: drive that are ordinarily susceptible to virus infection. This provides you with a basic level of protection that you can extend by configuring VirusScan to suit your own needs.

In its initial configuration, the program will prompt you for a response when it finds a virus (Figure 4-2).

Figure 4-2. VirusScan response options

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

- **Continue.** Click this to proceed with the scan operation and have VirusScan list each infected file in the lower portion of its main window (Figure 4-3), record each detection in its log file, but take no other action to respond to the virus. Once VirusScan has finished examining your system, you can right-click each file listed in the main window, then choose an individual response from the shortcut menu that appears.

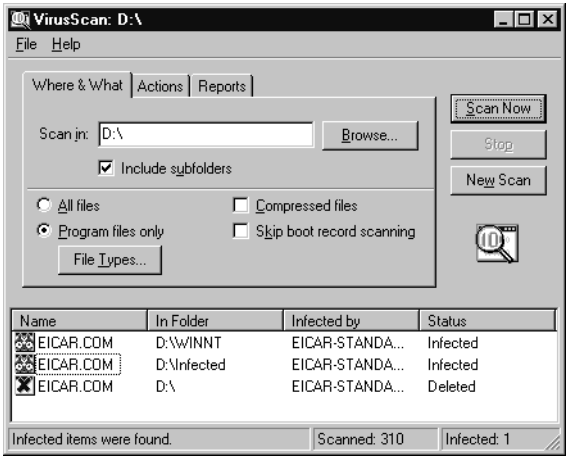


Figure 4-3. VirusScan main window

- **Stop.** Click this to stop the scan operation immediately. VirusScan will list the infected files it has already found in the lower portion of its main window (see Figure 4-3 on page 76) and record each detection in its log file, but it will take no other action to respond to the virus. Right-click each infected file listed in the main window, then choose an individual response from the shortcut menu that appears.
- **Clean.** Click this to have VirusScan try to remove the virus code from the infected file. If it cannot clean the file—either because it has no remover or because the virus has damaged the file beyond repair—it will record the incident in its log file and suggest alternative responses. In the example shown in Figure 4-2 on page 76, VirusScan failed to clean the mock EICAR test "virus." Here, **Clean** is not an available response option. In most cases, you should delete such files and restore them from backups.
- **Delete.** Click this to delete the file from your system immediately. By default, VirusScan will record the name of the infected file in its log so that you can restore the file from a backup copy.
- **Move file to.** Click this to open a dialog box that you can use to locate your quarantine folder, or another suitable folder. Once you have located the correct folder, click **OK** to transfer the file to that location.

IMPORTANT: If you *schedule* an on-demand scan operation, VirusScan will *not* prompt you to choose a response. Instead, you must choose an automatic response for it. See Chapter 6, "Scheduling and Running On-Demand Scan Operations," for more details.

By default, VirusScan simply continues the scan operation and records the results in its activity log file.

Understanding false detections

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

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

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

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

Using the On-Access Scanner 5

Scanning continuously

VirusScan uses its on-access scanning component to provide your workstation with continuous, real-time virus detection and response. The on-access scanner checks for infections each time you open or copy a file from, save a file to, or otherwise use any file stored on your workstation. It starts when you start your workstation, and stays in memory until you shut down. You can use the VirusScan On-Access Monitor that appears in the AntiVirus Console window to configure this scanner.

Configuring the on-access scanner

To ensure its optimal performance on your computer or in your network environment, you need to tell VirusScan what you want it to scan, what you want it to do if it finds a virus, and how it should let you know when it has.

By default, the on-access scanner simply looks for viruses on your workstation and notifies you when it finds one. It also records the incident in its log file. You can give the on-access scanner much more robust response options that protect your workstation automatically.

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

1. Start the AntiVirus Console. See "Starting the VirusScan AntiVirus Console" on page 51 to learn how to do so.

2. The VirusScan On-Access Monitor appears in the AntiVirus Console window (Figure 5-1).

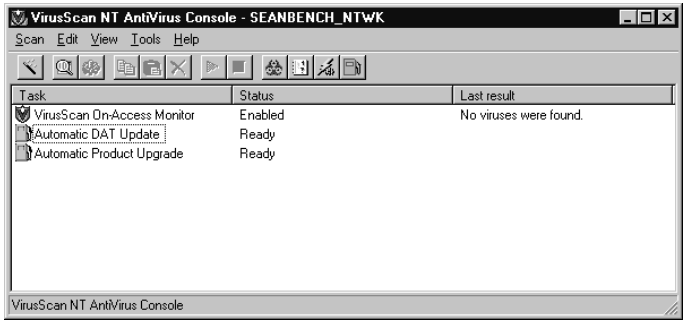


Figure 5-1. AntiVirus Console window

3. Select the On-Access Monitor in the Console window, then choose **Properties** from the **Scan** menu, or click  in the Console toolbar.

4. The VirusScan Properties dialog box appears (Figure 5-2).

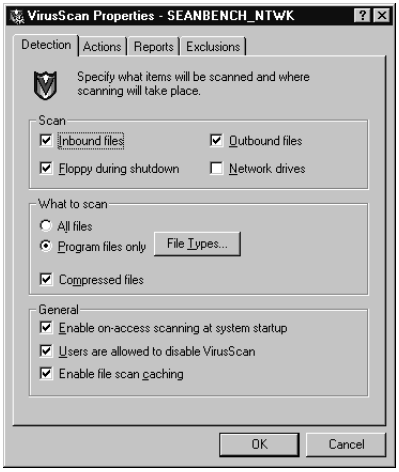


Figure 5-2. VirusScan Properties dialog box - Detection page

The VirusScan 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 VirusScan 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.

Choosing Detection options

Use the Detection page (Figure 5-2) to define the scope of the on-access scan operation—which file traffic VirusScan should examine 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 VirusScan to examine. Your choices are:

   - **Inbound Files.** Select this checkbox to scan all files written to or modified on your workstation.
   - **Outbound Files.** Select this checkbox to scan files read from your workstation.

- **Floppy during shutdown.** Select this checkbox to scan any floppy disk left in your drive as you shut down your workstation.
- **Network drives.** Select this checkbox to scan any network drive you have mapped to your workstation. This option will also scan any network drive you have currently open on your workstation, whether you mapped the drive or designated it with a Universal Naming Convention (UNC) path.

2. Specify which of the files in each traffic stream you want VirusScan to examine. Your choices are:

   - **All Files.** This tells VirusScan to scan all files stored on your workstation. 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 VirusScan will examine, click **File Types** to open the Program File Extensions dialog box.

     The Program File Extensions dialog box appears (Figure 5-3).

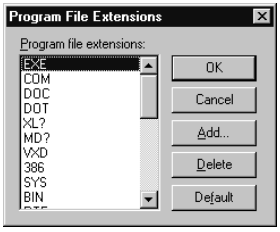


Figure 5-3. Program File Extensions dialog box

By default, VirusScan scans files with the extensions .EXE, .COM, .DOC, .DOT, .XL?, .MD?, .VXD, .386, .SYS, .BIN, .RTF, .OBD, .DLL, .SCR, .OBT, .PP? .POT, .OLE, .SHS, .MPP, .MPT, .XTP, .XLB, .CMD, .OVL, and .DEV. This list covers nearly all potentially susceptible files, including all Microsoft Office file types, which are susceptible to macro viruses. The ? character is a wildcard that enables VirusScan to examine files similar in type, such as document and template files.

  - To add to the list, click **Add**, then type the extension you want VirusScan 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.

- **Compressed files.** This tells VirusScan to look for viruses in files compressed with these formats: LZEXE, PKLite, .TD0, and .ZIP. Although it does give you better protection, scanning compressed files can lengthen a scan operation.

3. Choose general options that govern how the on-access scanner functions. Your choices are:

   - **Enable on-access scanning at system startup.** Select this checkbox to start the on-access service whenever you start your workstation.
   - **Users are allowed to disable VirusScan.** Select this checkbox to activate the **Disable** command in the on-access scanner's shortcut menu, the  button in the Console window's toolbar, and the **Disable** button in the VirusScan Statistics dialog box. Clearing this checkbox deactivates each of these commands and buttons.
   - **Enable file scan caching.** Select this checkbox to have the on-access scanner examine each file on your system once, when you first start your system or the Network Associates McShield service. The scanner then ignores the files it has scanned during later scan operations unless they get modified. This option can speed up scan operations considerably.

4. 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.**

Choosing Action options

VirusScan 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 VirusScan response that suits your working environment.

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.

   The VirusScan Properties dialog box appears. Click the Actions tab to display the correct property page (Figure 5-4).

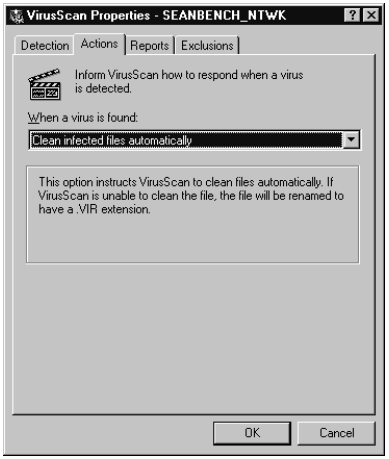


Figure 5-4. VirusScan Properties dialog box - Actions page

2. Choose the action VirusScan 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 VirusScan to deny network users access to any infected files it finds on the workstation. VirusScan will also append the extension .VIR to the names of any infected files. Be sure to enable VirusScan's logging option so that you have a record of which files are infected. See "Choosing Reports options" on page 84 for details.

   NOTE: Because VirusScan 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 workstation 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 VirusScan to move infected files to a "quarantine" folder. By default, VirusScan moves these files to a folder named Infected within its program directory. 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 VirusScan cannot move an infected file or cannot get access to it during a scan operation, it will append a .VIR extension to the file name and deny user access to it.

- **Clean infected files automatically.** This option tells VirusScan to try to remove the virus from the infected file.

  NOTE: If VirusScan cannot remove a virus from an infected file, or if the virus has damaged the file beyond repair, VirusScan will append a .VIR extension to the file name and deny user access to it. You should delete any such files and restore them from backups. Be sure to enable VirusScan's logging option so that you have a record of which files are infected. You can then restore damaged files from backup copies. See "Choosing Reports options" on page 84 for details.

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

3. 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.**

Choosing Reports options

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

The VirusScan 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 VirusScan 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 workstation.

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.

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

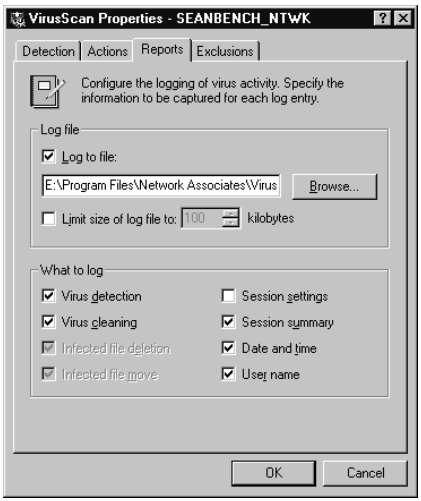


Figure 5-5. VirusScan Properties dialog box - Reports page

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

   By default, VirusScan writes log information to the file VIRUSSCAN ACTIVITY LOG.TXT in the VirusScan program directory. You can enter a different name in the text box provided, or click **Browse** to locate a suitable file elsewhere on your workstation 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, VirusScan does not limit the file size at all. If the data in the log file exceeds the file size you set, VirusScan erases the existing log file and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want VirusScan to record in its log file. The log options you see will depend on which options you chose in the Actions page. See "Choosing Action options" on page 83 for details.

You can choose to record this information:

- **Virus detection.** Select this checkbox to have VirusScan note how many infected files it found during this scanning session.
- **Virus cleaning.** Select this checkbox to have VirusScan note how many files it removed virus code from. This option will not be available if you do not choose **Clean infected files automatically** in the Actions page.
- **Infected file deletion.** Select this checkbox to have VirusScan note how many infected files it deleted from your system. This option will not be available if you do not choose **Delete infected files automatically** in the Actions page.
- **Infected file move.** Select this checkbox to have VirusScan note how many infected files it moved to your quarantine directory. This option will not be available if you do not choose **Move infected files to a folder** in the Actions page.
- **Session settings.** Select this checkbox to have VirusScan list the options you choose in the VirusScan Properties dialog box for each scanning session.
- **Session summary.** Select this checkbox to have VirusScan 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 VirusScan remained loaded into memory on your workstation. It ends when you either unload VirusScan or reboot your workstation.
- **Date and time.** Select this checkbox to have VirusScan append the date and time to each log entry it records.
- **User name.** Select this checkbox to have VirusScan append the name of the user logged in to the workstation at the time it records each log entry.

5. 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.**

Choosing Exclusion options

Many of the files stored on your workstation are not vulnerable to virus infection or never change. 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 VirusScan to look only at susceptible file types (see "Choosing Detection options" on page 80 for details), or you can tell VirusScan 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.

Next, 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.

   The VirusScan Properties dialog box appears. Click the Exclusions tab to display the correct property page. (Figure 5-6).

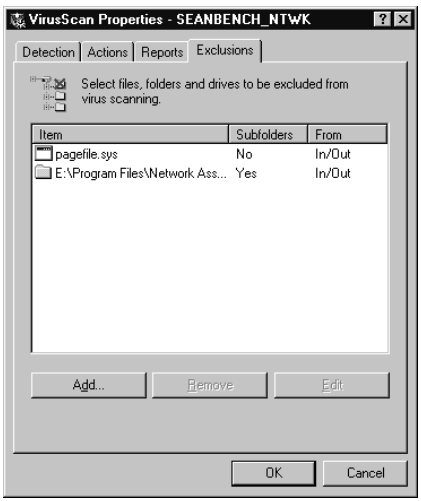


Figure 5-6. VirusScan Properties dialog box - Exclusions page

The Exclusions page will initially list a system database file and the VirusScan program directory. VirusScan excludes these files from scan operations because they are not susceptible to virus infection or because they are in almost constant use. The exclusion list also shows whether the scan operation is set to ignore all subfolders within the excluded item, and under which circumstances VirusScan excludes it.

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 5-7).

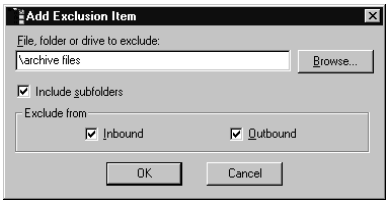


Figure 5-7. Add Exclusion Item dialog box

     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 workstation.

     NOTE: If you have VirusScan 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 VirusScan should exclude the file or folder as you or others save or copy it to your workstation, read it from your workstation, or both.

        – Select the **Inbound** checkbox to save the file or folder to your workstation without VirusScan scanning it.

        – Select the **Outbound** checkbox to read the file or folder from your workstation without VirusScan 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**. VirusScan will then scan this file or folder during its next on-access scanning operation.

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 and Running On-Demand Scan Operations 6

Initiating scan operations

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

The AntiVirus Console does not come with any pre-scheduled scan tasks because the variety of workstation setups and network environments within which VirusScan 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 66 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 54 for more details).

If you start VirusScan's stand-alone on-demand scanner, however, rather than running an on-demand task from the AntiVirus Console, you can scan your workstation's C: drive immediately. Simply click **Scan Now** when the main window appears. To learn more about this stand-alone scanner, see "Using the stand-alone on-demand scanner" on page 105.

Why run on-demand scan operations?

Because its on-demand scanner provides your workstation with background scanning protection, running on-demand scan operations might seem redundant. But good anti-virus security measures incorporate complete, regular system scans because:

- **Background scanning checks files as they execute.** VirusScan's on-access scanner looks for viruses as executable files run, or when you read a floppy disk. But on-demand scan operations can check for code signatures in files stored on your hard disk. If you rarely run an infected file, the on-access scanner might not detect the virus until it deploys its payload. An on-demand scan operation, however, can detect a virus as it waits for an opportunity to run.
- **Viruses are sneaky.** Accidentally leaving a floppy disk in your drive as you start your computer could load a virus into memory before the on-access service starts, particularly if you do not have the service configured to scan floppy disks. Once in memory, a potent virus can infect nearly any program.

- **On-access scanning takes time and resources.** Scanning for viruses as you run, copy or save files can delay, very slightly, software launch times and other tasks. Depending on your situation, this could be time you might rather devote to important work. Although the impact is very slight, you might be tempted to disable on-access scanning if you need every bit of available system power for demanding tasks. In that case, performing regular scan operations during idle periods can guard your system against infection without compromising performance.
- **Good security is redundant security.** In the networked, web-centric world in which most computer users operate today, it takes only a moment to download a virus from a source you might not even realize you visited. If a software conflict has disabled background scanning for that moment, or if background scanning is not configured to watch a vulnerable entry point, you could end up with a virus. Regular scan operations can often catch infections before they spread or do any harm.

Creating an on-demand task in the AntiVirus Console

The AntiVirus Console lists each of the on-demand tasks you have scheduled to run from your workstation. When you first start it, it comes with no pre-configured on-demand tasks. To create an entirely new on-demand task, follow these steps:

1. Start the AntiVirus Console (Figure 6-1). See "Starting the VirusScan AntiVirus Console" on page 51 to learn how to do so.

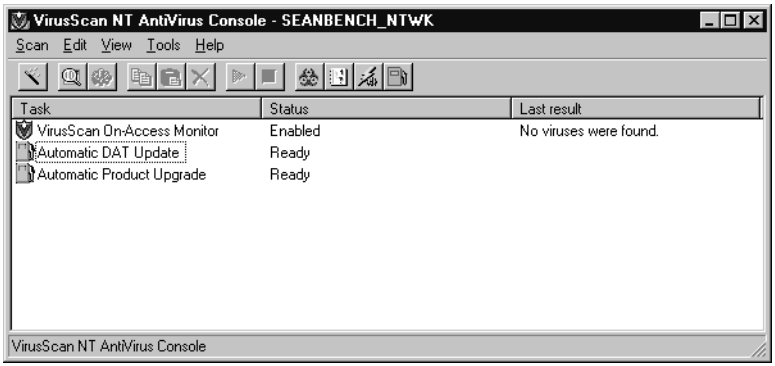


Figure 6-1. AntiVirus Console window

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

   A new on-demand task appears, highlighted, in the AntiVirus Console task window.

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

The Console opens the Task Properties dialog box (Figure 6-2).

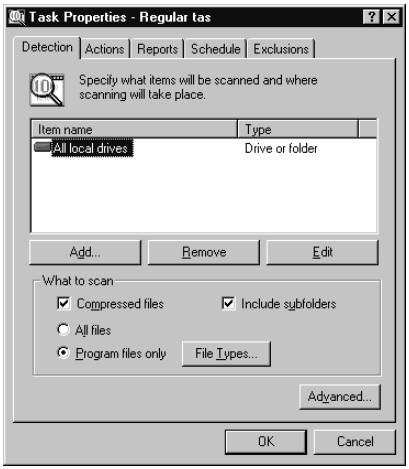


Figure 6-2. Task Properties dialog box - Detection page

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 VirusScan 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.

Choosing Detection options

Use the Detection page (Figure 6-2) to define the scope of the on-access scan operation—which drives, files, or folders VirusScan should scan for viruses and which file name extensions it should treat as susceptible to infection. By default, VirusScan lists all of the drives on your workstation 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 6-3).

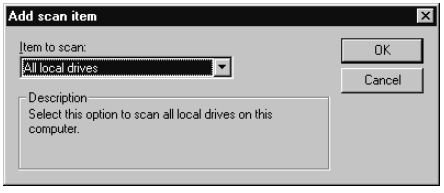


Figure 6-3. Add Scan Item dialog box

Next, choose a scan target from the list. You can choose to scan all local drives, particular drives or folder, or particular files. If you choose to scan a drive, folder, or file, enter its path 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 your workstation. When you have finished, click **OK** to close the dialog box.

- **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 6-4).

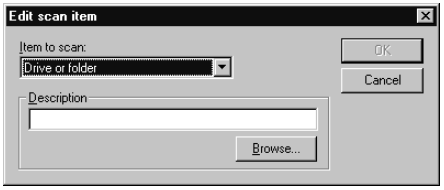


Figure 6-4. Edit Scan Item dialog box

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

2. Specify how you want VirusScan to conduct the scan. You can

   - **Scan volume subfolders.** By default, VirusScan 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, VirusScan scans files compressed with these formats: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, and .ZIP. Although it does give you better protection, scanning compressed files can lengthen a scan operation. You can prevent VirusScan from scanning these files 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 VirusScan will scan, click **File Types** to open the Program File Extensions dialog box (see Figure 6-5 on page 93).

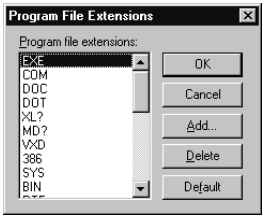


Figure 6-5. Program File Extensions dialog box

By default, VirusScan scans files with the extensions .EXE, .COM, .DOC, .DOT, .XL?, .MD?, .VXD, .386, .SYS, .BIN, .RTF, .OBD, .DLL, .SCR, .OBT, .PP? .POT, .OLE, .SHS, .MPP, .MPT, .XTP, .XLB, .CMD, .OVL, and .DEV. This list covers nearly all potentially susceptible files, including all Microsoft Office file types, which are susceptible to macro viruses. The ? character is a wildcard that enables VirusScan to examine files similar in type, such as document and template files.

- To add to the list, click **Add**, then type the extension you want VirusScan 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 workstation, 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 workstation operations, click **Advanced** to display the Advanced Scanner Settings dialog box (Figure 6-6).

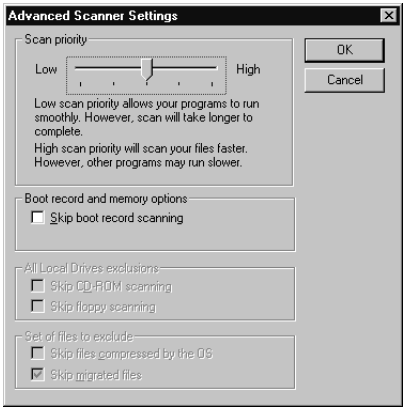


Figure 6-6. Advanced Scanner Settings dialog box

Your options are:

- **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 running on your workstation. This ensures that other running software 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 as you work.

  Drag the slider to the right to give the scan task more priority relative to other 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 you aren't working.

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

- **Skip boot record scanning.** VirusScan ordinarily will scan your master boot record and the boot blocks on your hard disk for boot-sector viruses. Although the majority of new viruses are macro viruses, boot sector viruses continue to spread and can cause your system harm. Network Associates recommends that you scan your boot record regularly, but if doing so will interfere with system operations, select this checkbox to bypass this type of scan operation.

- **Exclude CD-ROM volumes from scanning.** This option is not available in VirusScan for Windows NT.

- **Exclude file sets from scanning.** This option is not available in VirusScan for Windows NT.

- **Skip migrated files.** This option is not available in VirusScan for Windows NT.

When you have finished setting priorities 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**.

Choosing Actions options

VirusScan 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 VirusScan response that suits your working environment.

To choose how you want VirusScan to respond to viruses, 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 Task Properties dialog box appears. Click the Actions tab to display the correct property page. (Figure 6-7).

Figure 6-7. Task Properties dialog box - Actions page

2. Choose the action you want VirusScan to take when it finds a virus. Your choices are:

   - **Continue Scanning.** This tells VirusScan 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, VirusScan will tell you that it has found a virus and will record the incident in its log. See "Choosing Reports options" on page 97 for details.
   - **Move infected file to a folder.** This option tells VirusScan to move infected files to a "quarantine" folder. By default, VirusScan moves these files to a folder named Infected within its program directory.

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

NOTE: If VirusScan 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, VirusScan will record the incident in its log. See Chapter 7, "Sending Alert Messages" and "Choosing Reports options" on page 97 for more information.

- **Clean infected file.** This option tells VirusScan to try to remove the virus from the infected file.

NOTE: If VirusScan cannot remove a virus from an infected file, or if the virus has damaged the file beyond repair, VirusScan 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, VirusScan will record the incident in its log. See Chapter 7, "Sending Alert Messages" and "Choosing Reports options" on page 97 for more information.

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

3. To have VirusScan 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 Chapter 7, "Sending Alert Messages," 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.**

Choosing Reports options

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

The VirusScan 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 VirusScan 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 workstation. Use the Reports property page to determine which information VirusScan will include in its log file.

To tell VirusScan what to record in its 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 Task Properties dialog box appears. Click the Reports tab to display the correct property page. (Figure 6-8).

Figure 6-8. Task Properties dialog box - Reports page

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

By default, VirusScan writes log information to the file SCAN ACTIVITY LOG.TXT in the VirusScan NT program directory. You can enter a different name in the text box provided, or click **Browse** to locate a suitable file elsewhere on your workstation 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 (100MB). VirusScan does not, by default, limit the file size at all. If the data in the log exceeds the file size you set, VirusScan 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 VirusScan to record in its log file. The log options you see will depend on which options you chose in the Actions page. See "Choosing Actions options" on page 95 for details. You can choose to record this information:

   - **Virus detection.** Select this checkbox to have VirusScan note how many infected files it found during this scanning session.
   - **Virus cleaning.** Select this checkbox to have VirusScan note how many files it removed virus code from. This option will not be available if you do not choose **Clean infected file** in the Actions page.
   - **Infected file deletion.** Select this checkbox to have VirusScan note how many infected files it deleted from your system. This option will not be available if you do not choose **Delete infected file** in the Actions page.
   - **Infected file move.** Select this checkbox to have VirusScan note how many infected files it moved to your quarantine directory. This option will not be available if you do not choose **Move infected file to a folder** in the Actions page.
   - **Session settings.** Select this checkbox to have VirusScan list the options you choose in the VirusScan Properties dialog box for each scanning session.
   - **Session summary.** Select this checkbox to have VirusScan 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 VirusScan remained loaded into memory on your workstation. It ends when you either unload VirusScan or reboot your workstation.

- **Date and time.** Select this checkbox to have VirusScan append the date and time to each log entry it records.
- **User name.** Select this checkbox to have VirusScan append the name of the user logged in to the workstation 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.**

Choosing Schedule options

VirusScan provides you with tools to schedule scan operations at particular dates and times, or at particular intervals. You can schedule VirusScan to run a scan operation in your absence or at your convenience.

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 VirusScan Properties dialog box appears. Click the Schedule tab to display the correct property page. (Figure 6-9).

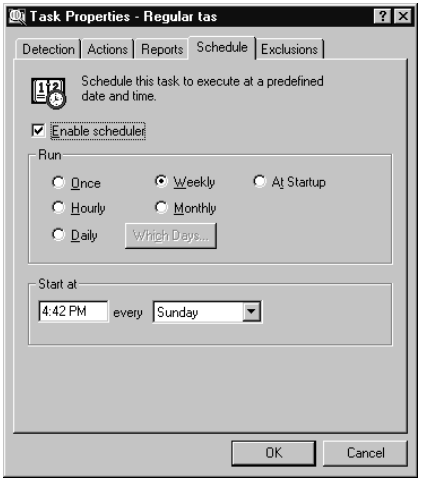


Figure 6-9. The Task Properties dialog box - Schedule page

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 VirusScan 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 workstation is active and VirusScan is running. Specify in the text box provided how many minutes VirusScan 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 VirusScan to run your task, your workstation must be active and VirusScan must be running. If your workstation is down or if VirusScan is not running at the time your task should start, the task will start at the next scheduled time.

Choosing Exclusions options

Many of the files stored on your workstation are not vulnerable to virus infection or never change. 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 VirusScan to look only at susceptible file types (see "Choosing Detection options" on page 91 for details), or you can tell VirusScan 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 VirusScan'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 workstation, however, provide you with the best virus defense.

To exclude files, folders, or volumes from on-demand 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 VirusScan Properties dialog box appears. Click the Exclusions tab to display the correct property page. (Figure 6-10).

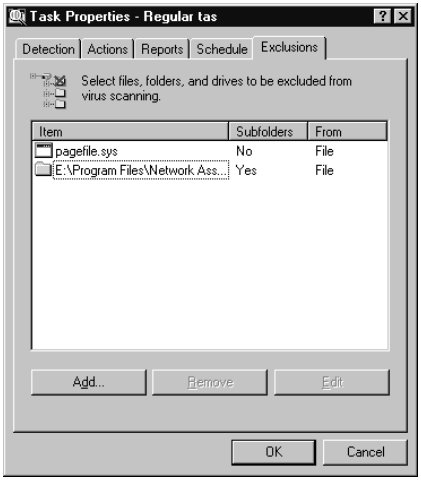


Figure 6-10. Task Properties dialog box - Exclusions page

The Exclusions page will initially list a system database file and the VirusScan program directory. VirusScan excludes these files from scan operations because they are not susceptible to virus infection or because they are in almost constant use. The exclusion list also shows whether the scan operation is set to ignore all subfolders within the excluded item, and under which circumstances VirusScan excludes it.

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 6-11).

Figure 6-11. Add Exclusion 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 workstation.

     NOTE: If you have VirusScan 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 VirusScan should exclude the file or folder from file scanning. Although you cannot scan your workstation's master boot record or boot blocks during a scheduled scan operation, you can configure an on-demand task that will do so with the stand-alone on-demand scanner. See "Using the stand-alone on-demand scanner" on page 105 for details.

     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**. VirusScan will then scan this file or folder during its next on-demand 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 close the AntiVirus Console and allow the task to run unattended. If you scheduled your task to run at a certain time, the Network Associates Task Manager service will start your task when you specified, provided that your workstation is active and VirusScan is running. If you have not scheduled your task but plan to run it immediately, you should probably leave the AntiVirus Console open 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. See "Starting the VirusScan AntiVirus Console" on page 51 to learn how to do so.

2. Select your on-demand task in the task list (Figure 6-12), then choose **Start** from the **Scan** menu, or click  in the Console toolbar.

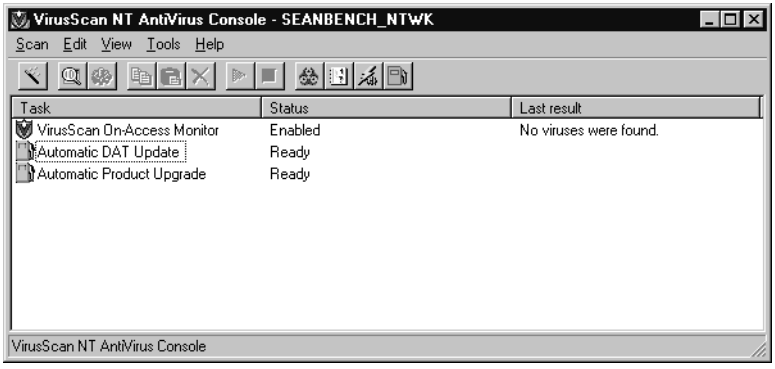


Figure 6-12. AntiVirus Console window

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 VirusScan 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. See "Starting the VirusScan AntiVirus Console" on page 51 to learn how to do so.

2. Double-click your on-demand task in the task list (see Figure 6-12 on page 103), or choose **Statistics** from the **Scan** menu, to open the Task Statistics dialog box (Figure 6-13).

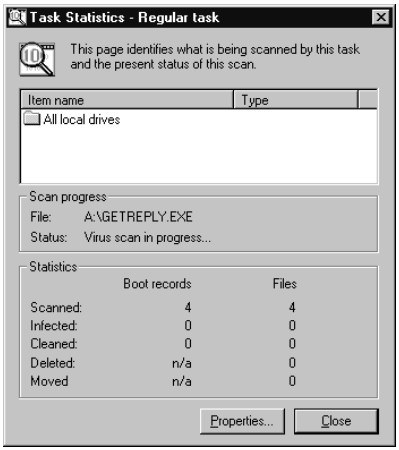


Figure 6-13. Task Statistics dialog box

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 VirusScan 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 90 to 103 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 the stand-alone on-demand scanner

When you schedule or run an on-demand scan operation from the AntiVirus Console, the Network Associates Task Manager service starts VirusScan (SCAN32.EXE) to conduct the scan operation. You can open this same program as a stand-alone scanner to conduct your own on-demand scan operations on the fly, or to choose exportable settings that you can send to other workstations on your network.

Some of the configuration options available through this interface also differ from those available when you configure a scan task through the AntiVirus Console.

Starting VirusScan

To start VirusScan, either

- Click **Start** in the Windows taskbar, point to **Programs**, then to **Network Associates VirusScan NT**. Next, choose **VirusScan** from the list that appears; or
- Click **Start**, then choose **Run** from the menu that appears. Type SCAN32.EXE in the Run dialog box, then click **OK**.

Both methods open the VirusScan window (Figure 6-14).

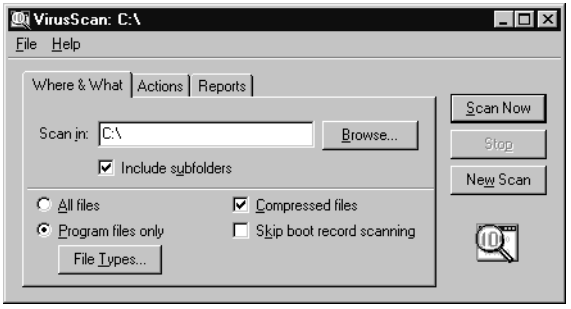


Figure 6-14. VirusScan main window

Click **Scan Now** at the right of the window to start the default scan task immediately, or configure a scan task that suits your needs by clicking the tabs at the top of the window and choosing options in each property page.

Using VirusScan menus

The menus along the top of the VirusScan window allow you to change some aspects of the program's operation. You can:

- **Start a scan operation.** Choose **Start** from the **File** menu to run a scan operation immediately, with whatever configuration options you have set currently. You can also click **Scan Now** to start a scan operation in the same way.

- **Save new settings.** By default, VirusScan will look for viruses in those files most susceptible to virus infection. It will scan your computer's master boot record and boot blocks, examine your C: drive and all of its subfolders, then pass a message to Alert Manager if it detects a virus. In this initial configuration, it will not take any action against any viruses it finds, but it will record its actions and summarize its current settings in a log file that you can review later.

  If you need different VirusScan configurations in order to run various scan operations, or if you want to run a scan operation with the same configuration on more than one computer, you can save your configuration options as a .VSC file with its own name. A .VSC file is a text file that records VirusScan configuration options, much like Windows .INI files record program startup options.

  To save your settings, first configure VirusScan with the options you want, then choose **Save Settings** from the **File** menu. Type a descriptive name in the Save As dialog box, choose a location for the file on your hard disk, then click **Save**. You can then copy this file to any other computer that should also use those settings. See "Configuring VirusScan" on page 108 for more details.

  To run VirusScan with these settings, simply locate and double-click the .VSC file you saved. This will start VirusScan with the settings loaded.

- **Open the VirusScan activity log.** Choose **View Activity Log** from the **File** menu to open the log file VirusScan uses to record its actions and settings.

  The log file will open in a Notepad window (see Figure 6-15 on page 107). You can print, edit, copy or otherwise treat this file as you would any ordinary text file. To learn more about what information the log file records, see "Choosing Reports options" on page 112.

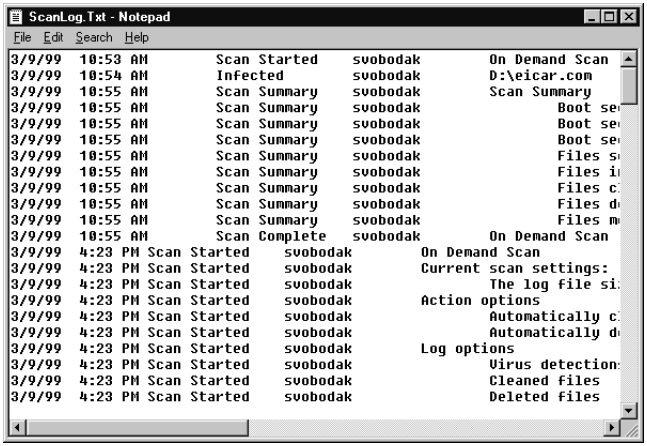


Figure 6-15. VirusScan Activity Log

- **Quit VirusScan.** Choose **Exit** from the **File** menu to quit VirusScan. Quitting VirusScan stops any active scan operations, but does *not* affect the Network Associates Task Manager or the on-access scanner's continuous background operations. Unless you save them, any configuration options you chose will also disappear when you quit VirusScan.

- **Connect to the online Virus Information Library.** Choose **Online Virus Info Library** from the **Help** menu will connect you to the Network Associates online Virus Information Library, provided you have an Internet connection and web browsing software available on your computer (Figure 6-16).

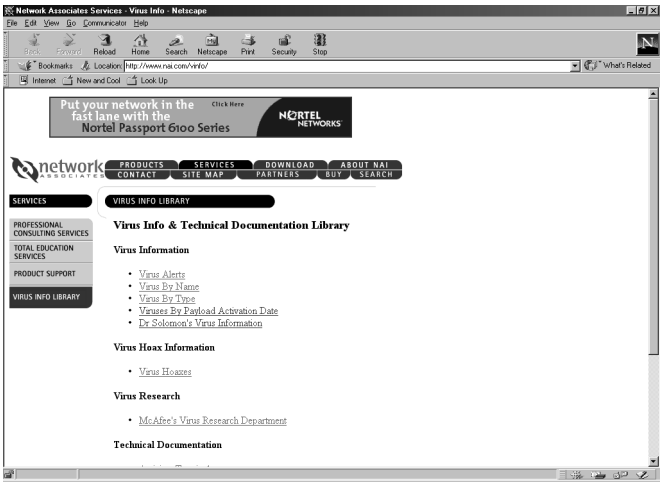


Figure 6-16. Online Virus Information Library

The Virus Information Library contains documents that give a detailed overview of each virus that VirusScan can detect or clean. That information includes how the virus infects and alters files, the sorts of payloads it deploys, how to recognize an infection, and other data. The Library also gives tips on preventing virus infection and removing viruses that VirusScan cannot remove from infected files.

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

Configuring VirusScan

To perform a scan operation, VirusScan needs to know what you want it to scan, what you want it to do if it finds a virus, and how it should let you know when it has. You can also tell VirusScan to keep a record of its actions. A series of property pages controls the options for each task—click each tab in the VirusScan window to set up VirusScan for your task.

Choosing Where & What options

VirusScan initially assumes that you want to scan your C: drive and all of its subfolders, and to restrict the files it scans only to those susceptible to virus infection (Figure 6-17).

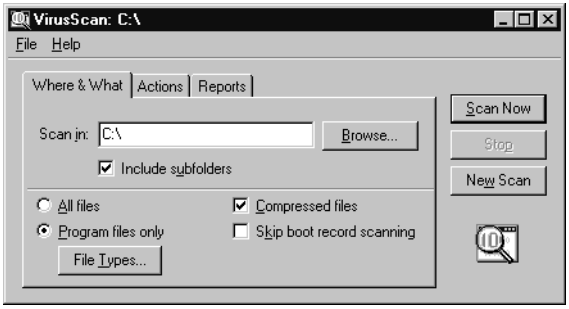


Figure 6-17. VirusScan main window - Where & What page

To modify these options, follow these steps:

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

   You can type a path to the target volume or folder in the **Scan in** text box, or click **Browse** to open the Browse for Folder dialog box (Figure 6-18).

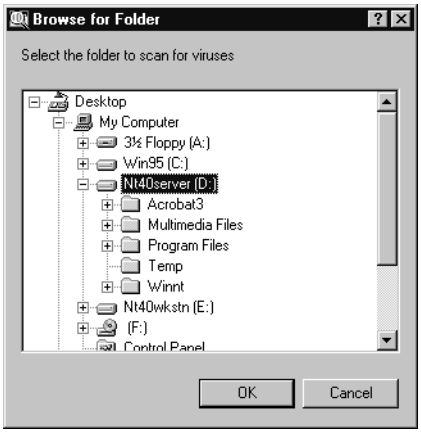


Figure 6-18. Browse for Folder dialog box

   Click ⊞ to expand the listing for an item shown in the dialog box. Click ⊟ to collapse an item. You can select hard disks, folders or files as scan targets, whether they reside on your system or on other computers on your network. You cannot select My Computer, Network Neighborhood, or multiple volumes as scan targets—to do so, you must create a scan task in the AntiVirus Console.

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

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

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

   - **Scan compressed files.** Select the **Compressed files** checkbox to have VirusScan look for viruses in files compressed with these formats: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, and .ZIP. Although it does give you better protection, scanning compressed files can lengthen a scan operation. You can prevent VirusScan from scanning these files by clearing the **Compressed files** checkbox.

- **Skip boot record scanning.** VirusScan ordinarily will scan your master boot record and the boot blocks on your hard disk for boot-sector viruses. Although the majority of new viruses are macro viruses, boot sector viruses continue to spread and can cause your system harm. Network Associates recommends that you scan your boot record regularly, but if doing so will interfere with system operations, select this checkbox to bypass this type of scan operation.

- **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** button. To see or designate the file name extensions VirusScan will examine, click **File Types** to open the Program File Extensions dialog box (Figure 6-19).

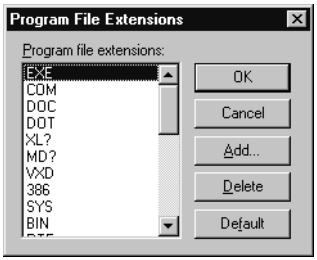


Figure 6-19. Program File Extensions dialog box

By default, VirusScan scans files with the extensions .EXE, .COM, .DOC, .DOT, .XL?, .MD?, .VXD, .386, .SYS, .BIN, .RTF, .OBD, .DLL, .SCR, .OBT, .PP? .POT, .OLE, .SHS, .MPP, .MPT, .XTP, .XLB, .CMD, .OVL, and .DEV. This list covers nearly all potentially susceptible files, including all Microsoft Office file types, which are susceptible to macro viruses. The ? character is a wildcard that enables VirusScan to examine files similar in type, such as document and template files.

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

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

To have VirusScan examine all files on your system, whatever their extensions, select the **All files** button. This will slow your scan operations down considerably, but will ensure that your system is virus free.

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

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

Choosing Actions options

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

Follow these steps:

1. Click the Action tab in the VirusScan window to display the correct property page (Figure 6-20).

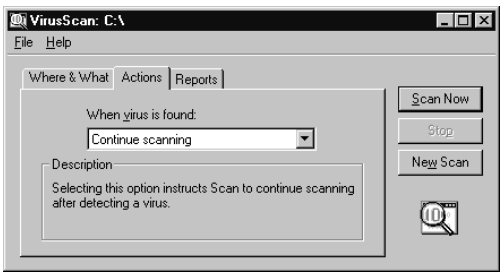


Figure 6-20. VirusScan window - Actions page

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

   - **Continue scanning.** Use this option only if you plan to leave your computer unattended while VirusScan checks for viruses. If you also activate the VirusScan reporting feature (see "Choosing Reports options" on page 112 for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

- **Prompt for action.** Choose this response if you expect to be at your computer when VirusScan scans your disk—VirusScan will display an alert message when it finds a virus and offer you the full range of its available response options.
- **Move infected files to a folder**. Choose this response to have VirusScan move infected files to a quarantine directory as soon as it finds them. By default, VirusScan moves these files to a folder named Infected within its program directory.

  You can enter a different name in the text box provided, or click **Browse** to locate a suitable folder on your hard disk.
- **Clean infected file.** Choose this response to tell VirusScan to remove the virus code from the infected file as soon as it finds it. If VirusScan cannot remove the virus, it will note the incident in its log file. See "Choosing Reports options" on page 112 for details.
- **Delete infected file.** Use this option to have VirusScan delete every infected file it finds immediately. Be sure to enable its reporting feature so that you have a record of which files VirusScan deleted. You will need to restore deleted files from backup copies. If VirusScan cannot delete an infected file, it will note the incident in its log file.

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

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

Choosing Reports options

By default, VirusScan sends a Windows NT network message via Alert Manager when it finds a virus. You can use the Report page to prevent VirusScan from sending this message to Alert Manager or to add an alert message to the Virus Found dialog box that appears when VirusScan finds an infected file. This alert message can contain any information, from a simple warning to instructions about how to report the incident to a network administrator.

This same page determines the size and location of VirusScan's log file. By default, the program lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called SCANLOG.TXT. You can have VirusScan write its log to this file, or you can use any text editor to create a text file for VirusScan to use. You can then open and print the log file for later review from within VirusScan or from your text editor.

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

1. Click the Report tab in the VirusScan window to display the correct property page (Figure 6-21).

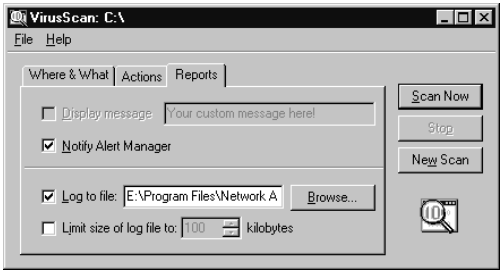


Figure 6-21. VirusScan main window - Reports page

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

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

     NOTE: To have VirusScan display your message, you must have selected **Prompt user for action** as your response in the Action page (see "Choosing Actions options" on page 111 for details).

   - **Send messages via Alert Manager.** Select the **Notify Alert Manager** checkbox to have VirusScan send alert information to Alert Manager for distribution. Alert Manager will notify you via whichever method you've configured it to use.

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

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

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

   Enter a value between 10KB and 99,999KB (100MB). By default, VirusScan does not limit the file size at all. If the data in the log exceeds the file size you set, VirusScan erases the existing log and begins again from the point at which it left off.

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

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

Sending Alert Messages 7

Using VirusScan's Alerting Features

Once you configure it with the options you want, you can let VirusScan 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 VirusScan 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 VirusScan 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.

VirusScan 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 138 to learn how to create or modify alert messages that suit your needs.

Configuring Alert Manager

VirusScan uses the Network Associates Alert Manager utility to notify you or others when it detects a virus on your workstation. 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 or servers on your network, you can also forward alert messages to those computers, which can in turn notify still other computers, in accordance with your network setup.

TIP: 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.

Although VirusScan can send messages to a centralized alerting system, it does *not* receive or process such alerts. NetShield NT—VirusScan's companion product for Windows NT Server—does, however. Consult your sales representative for details.

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 VirusScan AntiVirus Console" on page 51.

   The Alerts Properties page appears (Figure 7-1).

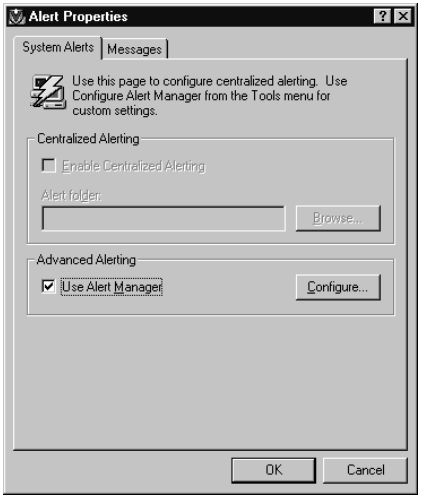


Figure 7-1. Alert Properties dialog box - System Alerts page

2. Make sure the **Use Alert Manager** checkbox is selected, then click **Configure** to open the Alert Manager dialog box (see Figure 7-2 on page 117).

   NOTE: VirusScan does not support the Centralized Alerting function shown here. This function is available in NetShield NT, VirusScan's companion product for Windows NT Server.

3. The Alert Manager dialog box includes 10 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 **Apply** to save your changes without closing the Alert Manager dialog box. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

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

   The following sections describe the options available for each method.

Viewing the Summary page

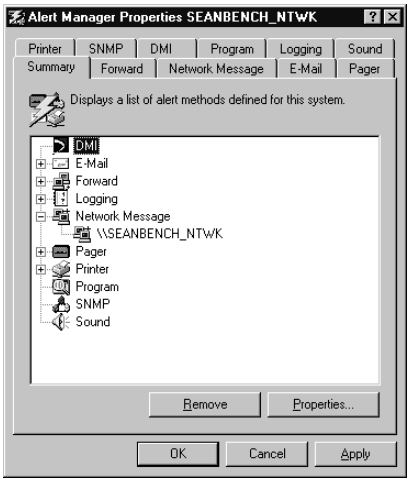


Figure 7-2. Alert Manager Properties dialog box - Summary page

The Summary page lists all of the alert methods you've configured VirusScan to use. In the example shown in Figure 7-2, Alert Manager has all 10 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, e-mail addresses, or other methods by which you will receive VirusScan alert messages. 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 method.

Forwarding alert messages to other computers

Alert Manager can forward the alert messages that VirusScan 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 7-3) appears with a list of all of the computers you have designated to receive forwarded messages. If you have not yet chosen any destination computers, this list will be blank.

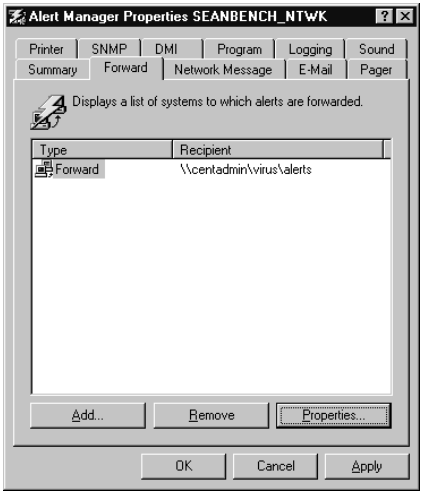


Figure 7-3. Alert Manager Properties dialog box - Forward page

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 7-4 on page 119), then enter in the text box provided the name of the computer that will receive the messages you forward. 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 7-4 on page 119). 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.

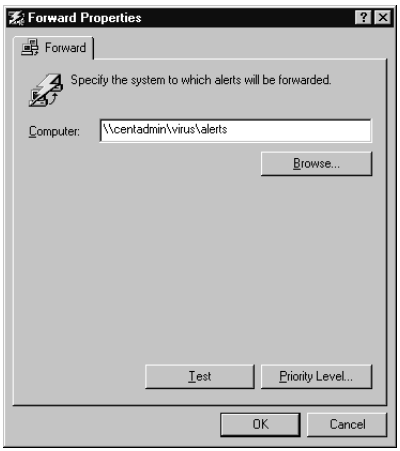


Figure 7-4. Forward Properties dialog box

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 7-5), 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. To learn how to set priority levels for different message types, see "Customizing alert messages" on page 138.

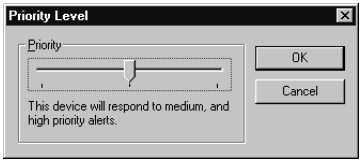


Figure 7-5. Priority Level dialog box

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. 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 changes without closing the Alert Manager dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

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

Sending alerts as a network messages

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

Destination computers must have the Windows NT 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 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 7-6). If you have not yet chosen a destination computer or a user, this list will be blank.

Figure 7-6. 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 7-7), 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 destination you specify is both a user name and a computer, Alert Manager will send the message to the user.

   - **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 7-7). Change any of the information you want to change in the Computer text box, then continue with Step 4.

Figure 7-7. 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 7-5 on page 119), 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.

   To learn how to set priority levels for different message types, see "Customizing alert messages" on page 138.

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. The recipient will need to click **OK** to acknowledge it. If your recipient does not receive the message, check the Windows NT Event Viewer 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 changes without closing the Alert Manager dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

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

Sending alert messages to e-mail addresses

Alert Manager can send the alert messages that VirusScan generates to a recipient's e-mail address via standard, Simple Mail Transfer Protocol (SMTP) e-mail services. 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 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 (Figure 7-8). If you have not yet chosen an e-mail address, this list will be blank.

Figure 7-8. 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 (Figure 7-9). Enter the e-mail address for your 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*> (admin@mydomain.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 7-9). 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 7-9. 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 7-5 on page 119), 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.

   To learn how to set priority levels for different message types, see "Customizing alert messages" on page 138.

5. Click **Mail Settings** to specify the SMTP server you use to send Internet mail. In the dialog box that appears (Figure 7-10), enter the server name in the Server text box and, in the Login text box, a user name for an active mail account that VirusScan can use to log on to the server.

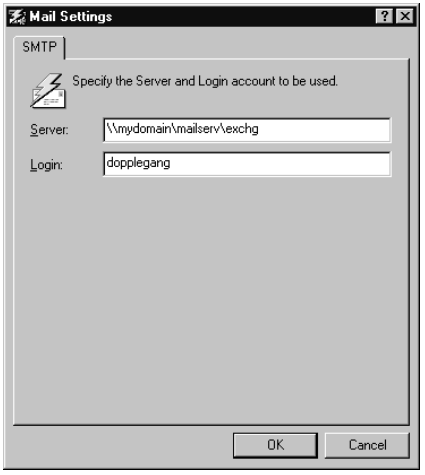


Figure 7-10. Mail Settings dialog box

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 changes without closing the Alert Manager dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

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

Sending alert messages to pagers

Alert Manager can send the alert messages that VirusScan generates to a recipient's pager, provided that you have a modem and telephone line connected to your workstation. 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 VirusScan can deliver its message.

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 (Figure 7-11) 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.

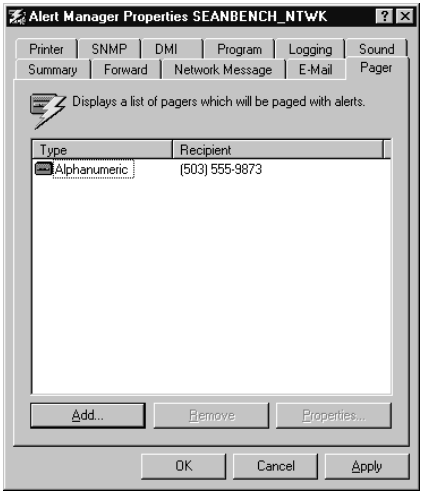


Figure 7-11. Alert Manager Properties dialog box - Pager page

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 7-12 on page 126). 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 VirusScan'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 7-12). 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.

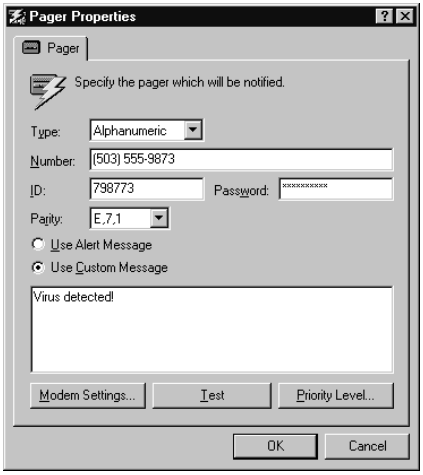


Figure 7-12. Pager Properties dialog box

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

In the Priority Level dialog box (see Figure 7-5 on page 119), 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.

To learn how to set priority levels for different message types, see "Customizing alert messages" on page 138.

5. Click **Modem Settings** to configure your modem to send pager messages. In the dialog box that appears (Figure 7-13), 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.

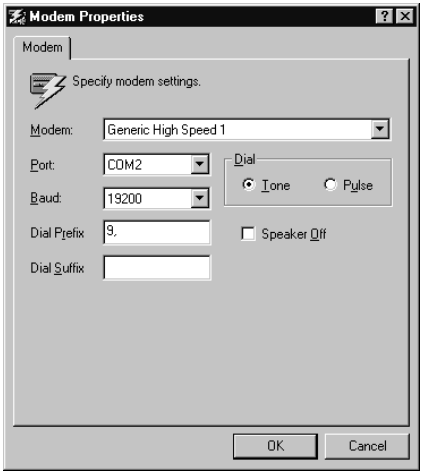


Figure 7-13. Modem Properties dialog box

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.

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 changes without closing the Alert Manager dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

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

Sending alert messages to a printer

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

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

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

   The Printer page (Figure 7-14) appears with a list of all of the printers you've set up to receive alert messages. If you have not yet chosen a printer, this list will be blank.

Figure 7-14. Alert Manager Properties dialog box - Printer page

3. To update this list, you can:

   - **Remove a listed printer.** Select one of the printers listed, then click **Remove.**
   - **Add a printer to the list.** Click **Add** to open the Printer Properties dialog box (see Figure 7-15 on page 129), then enter in the text box provided the name of the target printer, or click **Browse** to locate the printer 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 (Figure 7-15). 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 7-15. 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 7-5 on page 119), 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.

   To learn how to set priority levels for different message types, see "Customizing alert messages" on page 138.

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 changes without closing the Alert Manager dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

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

Sending alert messages via SNMP

Alert Manager can send the alert messages that VirusScan generates to other computers via the Simple Network Management Protocol (SNMP). To see the alert messages that VirusScan 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 viewer, see the documentation for your management software.

To configure VirusScan 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 7-16) appears.

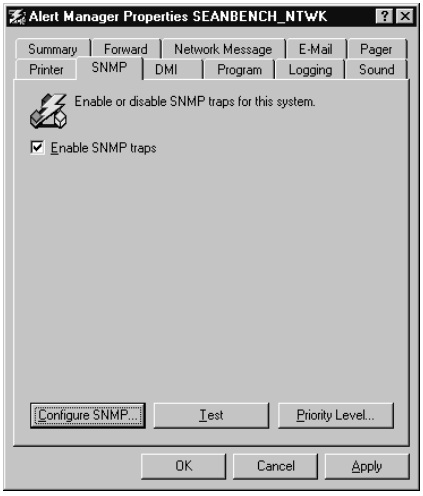


Figure 7-16. Alert Manager Properties dialog box - SNMP page

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 7-5 on page 119), 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 Alert Manager Properties dialog box.

   To learn how to set priority levels for different message types, see "Customizing alert messages" on page 138.
5. To activate SNMP alerting, you must install and activate SNMP on your workstation. If you have not yet configured this service, click **Configure SNMP** to open the Windows NT Network control panel. Next, click the Services tab, then click **Add** to add the SNMP service. See your Windows NT documentation for additional configuration details.
6. Click **Test** to send the SNMP computer a test message.
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 changes without closing the Alert Manager dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

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

Sending alert messages via the Desktop Management Interface

Alert Manager can send the alert messages that VirusScan generates to other computers via the Desktop Management Interface (DMI) Component Interface layer. The Desktop Management Interface is a multi-platform standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them.

To use this alerting method, you must have DMI management software installed and configured on your network. Consult the documentation for your DMI software for additional details.

> **NOTE:** To learn more about the Desktop Management Interface standard, see the Desktop Management Task Force website at http://www.dtmf.org

To configure VirusScan to send alert messages via DMI, follow these steps:

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

   The DMI page (Figure 7-17) appears.

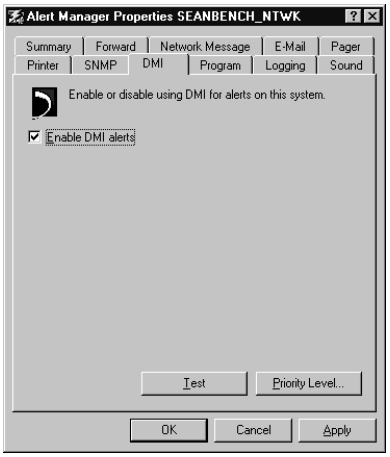


Figure 7-17. Alert Manager Properties dialog box - DMI page

3. Select the **Enable DMI alerts** checkbox.
4. Click **Priority Level** to specify which types of alert messages your DMI management software will receive.

   In the Priority Level dialog box (see Figure 7-5 on page 119), drag the slider to the right to send the DMI software fewer, but higher priority, messages. Drag the slider to the left to send the DMI software more alert messages, including lower priority messages. Next, click **OK** to save your changes and return to the Alert Manager dialog box.

   To learn how to set priority levels for different message types, see "Customizing alert messages" on page 138.

5. Click **Test** to send your DMI software a test 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 changes without closing the Alert Manager dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

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

Launching a program to send 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 VirusScan 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 execute a program when VirusScan finds a virus, follow these steps:

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

   The Program page (Figure 7-18) appears.

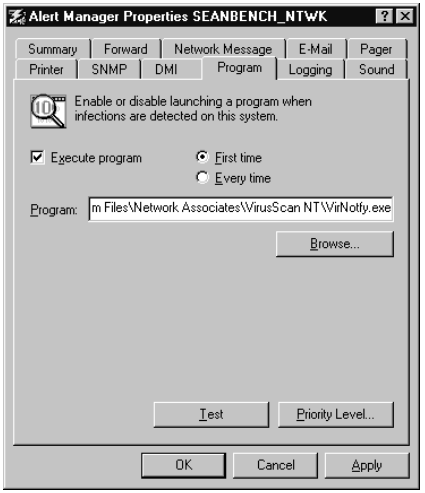


Figure 7-18. Alert Manager Properties dialog box - Program page

3. Enter the name and path of the program you want VirusScan to run when it finds a virus, or click **Browse** to locate the program file on the network.

   By default, Alert Manager runs the program VIRNOTFY.EXE from within the VirusScan program directory. This program runs without an interface, and takes input only from VirusScan via two variables:

   - %INFFILENAME% - This identifies the location of the infected file, including its path.
   - %VIRUSNAME% - This identifies the infecting virus.

It then displays the information VirusScan supplies in a Virus Notification dialog box that pops up on your workstation screen. You must click **OK** to close this dialog box before you can continue working.

> **NOTE:** If you prefer a different Virus Notification display, you can write your own display application or batch file that incorporates these variables.

4. To have VirusScan start the program only when it first finds a virus, select the **First Time** button. To start the program every time it finds a virus, select the **Every Time** button.

> **IMPORTANT:** If you select **First Time**, VirusScan will start the program you designate the first time it encounters any virus. If it finds more than one occurrence of that same 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, VirusScan will start the same program three times in a row. Starting multiple instances of the same program could cause your workstation 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 7-5 on page 119), drag the slider to the right to tell VirusScan to start the program in response to fewer, but higher priority, alert events. Drag the slider to the left to have VirusScan start the program more often, in response to lower priority alert events. Next, click **OK** to save your changes and return to the Alert Manager Properties dialog box.

   To learn how to set priority levels for different message types, see "Customizing alert messages" on page 138.

7. To test VirusScan's ability to start the program, click **Test.**

8. To configure other notification options, click a different tab. To save your changes without closing the Alert Manager dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

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

Sending alert messages to Windows NT system logs

Alert Manager can send the alert messages that VirusScan generates to the system log on any workstation or server that runs Windows NT. To view alert messages sent with this method, you must open the Windows NT Event Viewer. See your Windows NT documentation for details.

To send alert messages to a Windows NT system log, follow these steps:

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

   The Logging page (Figure 7-19) appears with a list of all of the computers you've set up to receive alert messages. If you have not yet configured any computers to receive alert messages, this list will be blank.

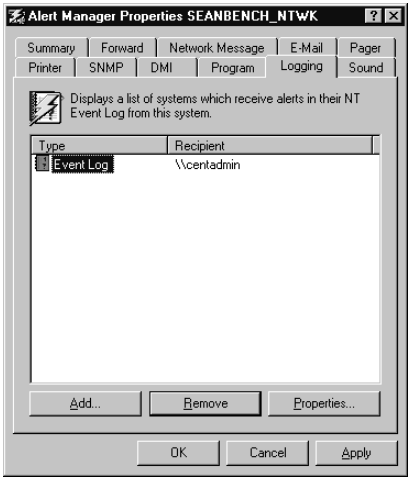


Figure 7-19. Alert Manager Properties dialog box - Logging page

3. To update this list, you can:
   - **Remove a listed computer.** Select one of the computers listed, then click **Remove.**
   - **Add a computer to the list.** Click **Add** to open the Logging Properties dialog box (see Figure 7-20 on page 136), then enter in the text box provided the name of the target computer, or click **Browse** to locate the computer on the network. To choose additional options, continue with Step 4.
   - **Change configuration options.** Select one of the computers listed, then click **Properties.** Alert Manager opens the Logging Properties dialog box (see Figure 7-20 on page 136). Change 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 7-20. Logging 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 (see Figure 7-5 on page 119), 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 network messages, including lower priority messages. Next, click **OK** to save your changes and return to the Logging Properties dialog box.

   To learn how to set priority levels for different message types, see "Customizing alert messages" on page 138.

5. Click **Test** to send the destination computer a test message. The message will appear in the target system's system log. Open the Windows NT Event Viewer to see the 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 changes without closing the Alert Manager dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

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

Sending an alert by playing a sound

Alert Manager can play a sound to alert you when it finds a virus. You can choose to play any sound formatted as a .WAV file, or you can have Alert Manager play a default “exclamation” sound.

To have VirusScan play a sound when it finds a virus, follow these steps:

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

   The Sound page (Figure 7-21) appears.

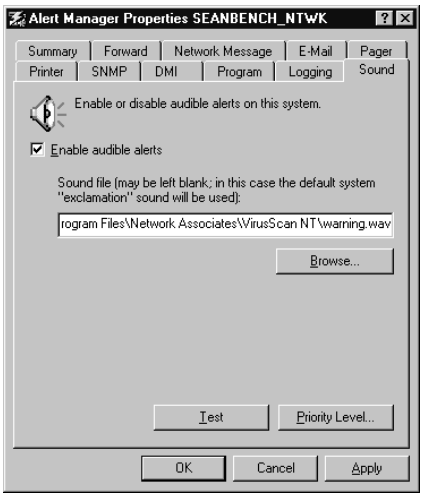


Figure 7-21. Alert Manager Properties dialog box - Sound page

3. Select the **Enable audible alerts** checkbox.
4. Enter the name and path to the sound file you want VirusScan to play when it finds a virus, or click **Browse** to locate the program file on your hard disk.

   By default, Alert Manager plays the sound WARNING.WAV from within the VirusScan program directory.
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 7-5 on page 119), drag the slider to the right to tell VirusScan to play a sound in response to fewer, but higher priority, alert events. Drag the slider to the left to have VirusScan play a sound more often, in response to lower priority alert events. Next, click **OK** to save your changes and return to the Alert Manager Properties dialog box.

   To learn how to set priority levels for different message types, see "Customizing alert messages" on page 138.

7. To test VirusScan's ability to play the sound you chose, click **Test.**

8. To configure other notification options, click a different tab. To save your changes without closing the Alert Manager dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

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

Customizing alert messages

VirusScan 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 workstation or elsewhere on your network. These alert messages come with a preset priority level. They also incorporate variables that identify the infected file and system, name the infecting virus, and provide 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. VirusScan 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 VirusScan 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, VirusScan comes with all of its alert messages enabled. To prevent VirusScan 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 7-1 on page 116). Click the Messages tab to display the correct property page (Figure 7-22).

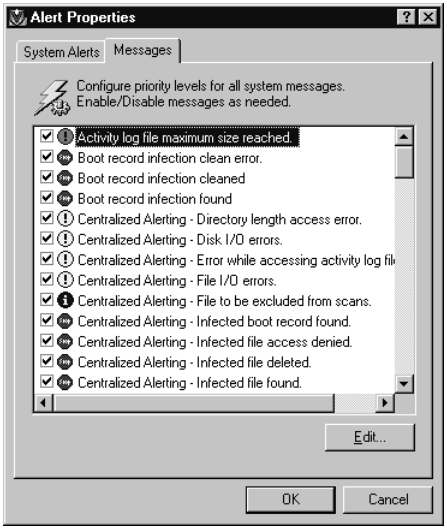


Figure 7-22. Alert Properties dialog box - Messages page

2. Review the list of messages shown. To disable those you do not want VirusScan to send, clear the checkbox at the left. Leave the checkbox selected beside those messages you *do* want VirusScan 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 VirusScan 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 VirusScan encounters a virus on your workstation than learn that the program excluded a certain file during a scan operation. By default, VirusScan assigns a priority level to each of its alert messages that reflects the urgency that 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 the most important ones 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 7-1 on page 116). Click the Messages tab to display the correct property page (see Figure 7-22 on page 139).

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

   The Configure System Message dialog box appears (Figure 7-23).

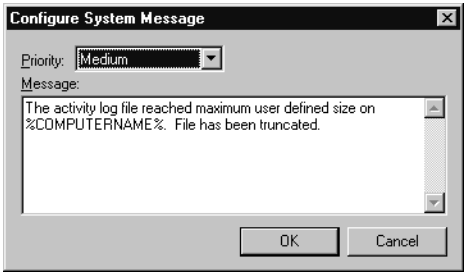


Figure 7-23. Configure System Message dialog box

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 VirusScan finds a virus on your server, but that you didn't want it to page you with routine operational messages. Instead, you'd rather have Alert Manager send the routine messages via e-mail or other, less urgent means.

   To do this, you would use the Messages pages in the Alert Properties dialog box to assign a high priority to virus alerts, and a medium or low priority to the routine messages (see Figure 7-22 on page 139). Next, you need to tell Alert Manager to send only high priority messages to your pager.

To do so, return to the Alert Manager dialog box (see Figure 7-2 on page 117), then click the tab for the alert method you want to modify. 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 (see Figure 7-5 on page 119).

Customizing alert messages

To help you respond to a situation that requires your attention, VirusScan 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 it to say, you should try to keep its essence intact, because VirusScan will send each message only when it encounters certain conditions. VirusScan 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 dialog box appears (see Figure 7-1 on page 116). Click the Messages tab to display the correct property page (see Figure 7-22 on page 139).

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

   The Configure System Message dialog box appears (see Figure 7-23 on page 140).

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

   VirusScan uses these variables in alert messages:

   - %FILENAME% - VirusScan 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% - VirusScan replaces this variable name with the name of an active task. This could include the name of the task that found a virus, or the name of a task that reported an error during a scan operation.

- %VIRUSNAME% - VirusScan replaces this variable name with the name of an infecting virus.
- %DATE% - VirusScan replaces this variable name with the date on which it performed a scan operation.
- %TIME% - VirusScan replaces this variable name with the time at which it performed a scan option.
- %COMPUTERNAME% - VirusScan 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 to which VirusScan connected.
- %SOFTWARENAME% - VirusScan 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 VirusScan interacted.
- %SOFTWAREVERSION% - VirusScan 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 VirusScan interacted.
- %USERNAME% - VirusScan replaces this variable name with the name of the user currently logged into your workstation. 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.

Updating and Upgrading VirusScan 8

Why update and upgrade?

To function at peak efficiency, VirusScan needs regular infusions of new virus definition data files (.DAT files), improvements to its scanning engine, and other technical enhancements. Without updated files, VirusScan might not detect new virus strains or respond effectively to remove the threat from your system. New viruses appear in various locations around the world at the rate of more than 200 per month—updating your virus definition files at least this often prevents unpleasant surprises.

Network Associates, through its NAI Labs division and its Anti-Virus Emergency Response Team (AVERT), releases new .DAT files every month to counter new virus strains; upgrade files arrive when changes in virus characteristics or product improvements warrant their release. The Automatic DAT Update and the Automatic Product Upgrade utilities that come with VirusScan make it easy to take advantage of this service. You can also install SecureCast, a Network Associates client service, to receive web-based update "broadcasts" as soon as new files become available.

NOTE: "Updating" VirusScan means downloading and installing new .DAT file versions; "upgrading" VirusScan means downloading and installing product version revisions, executables and, in some cases, .DAT files. Network Associates offers free .DAT file updates for the life of your product. This does not, however, guarantee that .DAT files will be compatible with previous product versions.

Your right to download free VirusScan upgrades depends on the terms of your license or on the terms of the sales contract you agreed to at the time of your purchase. If you have questions about these terms, consult the LICENSE.TXT or README.1ST documents included with your VirusScan copy, or consult your sales representative. Network Associates makes upgrade files available for you to download freely from its online services for as long as your license permits.

Update and upgrade strategies

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

Instead, Network Associates recommends that you use the Automatic DAT Update and Automatic Product Upgrade utilities in conjunction with their companion service SecureCast in an efficient "push-pull" arrangement. Once you install its client software on an administrative server, SecureCast can send, or "push," updated files to you automatically, as soon as NAI Labs makes them available. See "Setting up Enterprise SecureCast" on page 225 for more details.

If you then make these updated files available on one or more central servers on your network and configure your remaining network nodes to "pull" the updated files from those servers, you can:

- Schedule network-wide .DAT file roll-outs and product upgrades for convenient times and with minimal intervention from either administrators or network users. You can configure the automatic update and upgrade tasks to schedule a time for each network node to poll the server for updated files. You might, for example, stagger your update tasks, or set a schedule that phases in or rotates .DAT file updates and product upgrades among different parts of the network.
- Split roll-out administration duties among different servers or domain controllers, among different regions of wide-area networks, or across other network divisions. Keeping update and upgrade traffic primarily internal can also reduce the potential for network security breaches.
- Reduce the likelihood that you will need to wait to download new .DAT or upgrade files. Traffic on Network Associates servers increases dramatically on regular .DAT file publishing dates and whenever new product versions appear. Avoiding the competition for network bandwidth enables you to deploy your new software with minimal interruptions.

Other advanced updating options allow you to back up existing .DAT files, install the .DAT file update, or run particular programs after successful updates. A set of Automatic Update/Upgrade property pages controls the options for this task—see "Configuring Automatic DAT Update options" on page 145 and "Configuring Automatic Product Upgrade options" on page 150 for details.

Configuring Automatic DAT Update options

Revised virus definition files appear on the Network Associates FTP site as data file (.DAT) packages. A .DAT package consists of an archived .ZIP file named DAT-XXXX.ZIP. The XXXX in the file name is a series number that changes with each .DAT file release. The Automatic DAT Update utility downloads these files, stops VirusScan's on-access scanner temporarily, installs the revised files, then starts the on-access scanner again. VirusScan can then use the revised files immediately.

To configure the Automatic DAT Update task, follow these steps:

1. Start the AntiVirus Console. See "Starting the VirusScan AntiVirus Console" on page 51 to learn how to do so.
2. Select the Automatic DAT Update task, then click  in the Console toolbar to open the Automatic Update/Upgrade Properties dialog box (Figure 8-24).

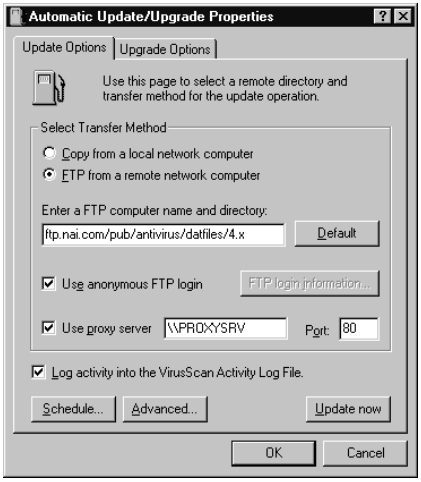


Figure 8-24. Automatic Update/Upgrade dialog box - Update Options page

3. To start an update task immediately, using the default configuration options already set for the task, simply click **Update now** at the bottom of the dialog box. Otherwise, continue with the next steps to change configurations or set an update schedule.

4. Choose the method you want to use to connect to the download server. Your choices are:

   - **Copy from a local network computer**. Select this option to simply transfer the update files from a computer somewhere on your network via whichever common network protocol you have active. The settings for this protocol will govern how the Automatic DAT Update task attempts the connection and the length of the timeout period that must pass before it stops the connection attempt.

     Enter the computer name in Universal Naming Convention (UNC) notation in the text box provided, or click **Browse** to locate the computer on your network. The remaining options in the Select Transfer Method area of the dialog box become unavailable.

     IMPORTANT: The Automatic DAT Update task expects to find new .DAT files in their original .ZIP archives and with their original file names. If you save the new files on a central server so that other workstations can download them, be sure that you do not extract the files or rename them.

     If you save your update files on a Novell NetWare server, you must install and use the File Copy utility in conjunction with the Automatic DAT Update utility. To learn how to install this utility, see Step 7 on page 35 in Chapter 2. To learn how the utility works, see "Updating and Upgrading from NetWare servers" on page 155.

   - **FTP from a remote network computer**. Select this option to transfer the update files via File Transfer Protocol (FTP). To use this option, the download server must have an FTP service enabled.

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

     Next, enter the domain name for the target server, together with any other necessary directory information, in the text box provided. Clicking **Default** enters the Network Associates FTP server:

     ftp://ftp.nai.com/pub/antivirus/datfiles/4.x

     If the target server accepts anonymous FTP logins, select the **Use anonymous FTP login** checkbox. If you use a specific FTP account that requires a user name and password, clear the checkbox, then click **FTP login information** instead. This button opens a dialog box where you can enter the correct user name and password. Enter the password again to confirm it, then click **OK** to close the dialog box.

5. If you route FTP requests from your network through a proxy server, select the **Use proxy server** checkbox, then enter the name of your proxy server in the text box provided. You can enter the name in UNC notation or as a domain name, whichever is appropriate for your environment. Next, in the remaining text box, enter the logical port for the proxy server you want to address with your FTP request.

6. To record the results of the update operation, select the **Log activity into the VirusScan Activity Log File** checkbox.

   By default, the log file records when an update task starts and how it finishes. To open and view the activity log, choose **Activity Log** from the **Scan** menu in the AntiVirus Console window.

7. Click **Schedule** to open a dialog box where you can set a one-time or recurring schedule for your update task (see Figure 8-25 on page 147).

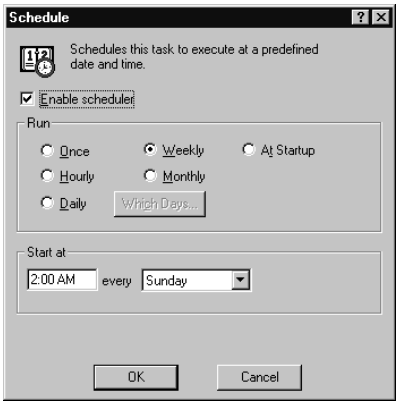


Figure 8-25. Schedule dialog box

8. Select the **Enable scheduler** checkbox. The options in the Run and the Start At areas will become active.

9. Choose how often you want the task to run in the Run area, or select **At Startup** to run your task as soon as VirusScan 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 workstation is active and VirusScan is running. Specify in the text box provided how many minutes VirusScan 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.

10. To save your changes and return to the Automatic Update/Upgrade Properties dialog box, click **OK**. To return to the dialog box without saving your changes, click **Cancel.**

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

11. To configure additional options, click **Advanced**, then see "Configuring advanced update options" to learn about your choices. To save your changes and return to the AntiVirus Console, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

Configuring advanced update options

To ready your update task to run, you need to enter only a target server, a connection method, and any necessary login information. Then, once you set a schedule for it, the Automatic DAT Update utility will download the correct files from the target server for you, extract them from their .ZIP archives, and install them into the VirusScan program directory.

To do additional pre- or post-processing on the files, or to take other actions, click **Advanced** to open the Advanced Update Options dialog box (see Figure 8-26 on page 149).

Figure 8-26. Advanced Update Options dialog box

Next, follow these steps:

1. Tell the Automatic DAT Update utility what you want it to do before or as it performs an update. Your options are:

   - **Backup the existing .DAT files.** Select this checkbox to have the utility rename existing VirusScan .DAT files before it installs new files. To rename each file, the utility appends the extension .SAV to the existing file name and extension. CLEAN.DAT, for example, will become CLEAN.DAT.SAV.
   - **Retrieve the Update file but do not perform the update**. Select this checkbox to have the utility download the .ZIP archive that contains the new .DAT files and simply save it in a location you specify instead of extracting it and installing it.

     ➧ **TIP:** Select this option if you plan to configure other workstations on your network to update from a central server.

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

2. Tell the Automatic DAT Update utility what you want it to do after it successfully downloads, extracts, and installs new .DAT files. Your options are:

   - **Save the Update file for later usage.** Select this checkbox to have the utility save an unextracted copy of the .DAT file package in a location you specify. After it saves a copy, the utility extracts the .DAT files from the update package and continues with the installation on the local workstation. By contrast, the **Retrieve the Update file but do not perform the update** option saves the unextracted file, but does not install the new .DAT files.

     TIP: Select this option if you plan to configure other workstations on your network to update from a central server.

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

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

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

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

Configuring Automatic Product Upgrade options

Network Associates revises VirusScan frequently to add new detection and repair capabilities, new features for manageability and flexibility, and other enhancements that make it a better anti-virus security tool.

VirusScan's Automatic Product Upgrade utility is designed specifically to look for and download these new versions as they become available. It connects automatically to a central server on your network or to a designated FTP site, downloads the new files, extracts and verifies them, backs up the existing files, then begins installing the new files. After it finishes, it starts all VirusScan services again and resumes its scan operations.

By default, the utility included with VirusScan does not come configured with the site information necessary to download new VirusScan versions. Registered VirusScan users can obtain this information from their sales representatives or from other Network Associates sources.

To configure the Automatic Product Upgrade task, follow these steps:

1. Start the AntiVirus Console. See "Starting the VirusScan AntiVirus Console" on page 51 to learn how to do so.
2. Select the Automatic Product Upgrade task, then click  in the Console toolbar to open the Automatic Update/Upgrade Properties dialog box (see Figure 8-24 on page 145).
3. Next, click the Upgrade Options tab to display the correct property page (Figure 8-27 on page 151).

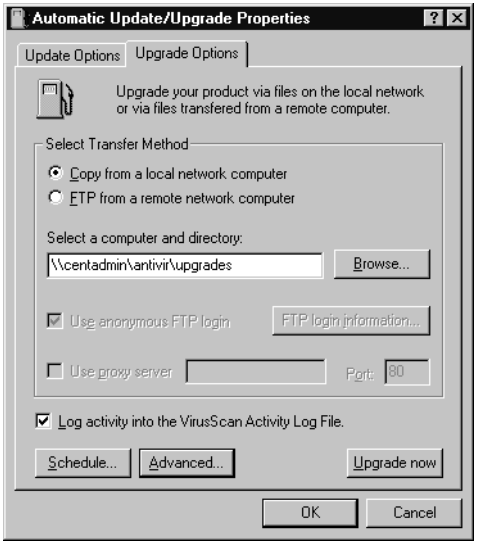


Figure 8-27. Automatic Update/Upgrade dialog box - Upgrade Options page

4. To start an upgrade task immediately, using the default configuration options already set for the task, simply click **Upgrade now** at the bottom of the dialog box. Otherwise, continue with the next steps to change configurations or set an update schedule.

5. Choose the method you want to use to connect to the download server. Your choices are:

   - **Copy from a local network computer**. Select this option to simply transfer the update files from a computer somewhere on your network via whichever common network protocol you have active. The settings for this protocol will govern how the Automatic Product Upgrade task attempts the connection and how long it will wait before it stops the connection attempt.

     Enter the computer name in Universal Naming Convention (UNC) notation in the text box provided, or click **Browse** to locate the computer on your network. The remaining options in the Select Transfer Method area of the dialog box become unavailable.

     IMPORTANT: The Automatic Product Upgrade task expects to find an *unzipped* disk image of the new upgrade files on your server. This allows you to customize your installation before deploying new files.

     If you save your update files on a Novell NetWare server, you must install and use the File Copy utility in conjunction with the upgrade utility. To learn how to install this utility, see Step 7 on page 35 in Chapter 2. To learn how it works, see "Updating and Upgrading from NetWare servers" on page 155.

     If you store upgrade files on a server that uses case-sensitive file names, you must rename the file PKGDESC.INI, which comes with VirusScan upgrades, so that it uses only lower-case letters. Otherwise, the upgrade utility will not find the file on the server and therefore will not install the new VirusScan version on client computers.

   - **FTP from a remote network computer**. Select this option to transfer the update files via File Transfer Protocol (FTP). To use this option, the download server must have an FTP service enabled.

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

     Next, enter the domain name for the target server, together with any other necessary directory information, in the text box provided.

If the target server accepts anonymous FTP logins, select the **Use anonymous FTP login** checkbox. If you use a specific FTP account that requires a user name and password, clear the checkbox, then click **FTP login information** instead. This button opens a dialog box where you can enter the correct user name and password. Enter the password again to confirm it, then click **OK** to close the dialog box.

6. If you route FTP requests from your network through a proxy server, select the **Use proxy server** checkbox, then enter the name of your proxy server in the text box provided. You can enter the name in UNC notation or as a domain name, whichever is appropriate for your environment. Next, in the remaining text box, enter the logical port for the proxy server you want to address with your FTP request.

7. To record the results of the upgrade operation, select the **Log activity into the VirusScan Activity Log File** checkbox.

   By default, the log file records when an upgrade task starts and how it finishes. To open and view the activity log, choose **Activity Log** from the **Scan** menu in the AntiVirus Console window.

8. Click **Schedule** to open a dialog box where you can set a one-time or recurring schedule for your upgrade task (Figure 8-28).

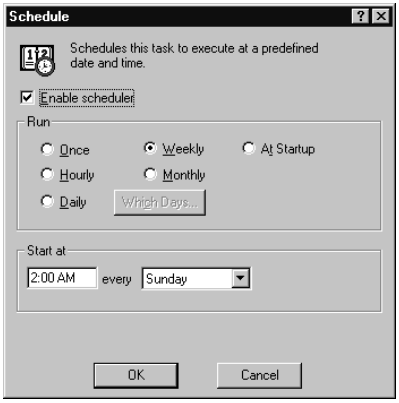


Figure 8-28. Schedule dialog box

9. Select the **Enable scheduler** checkbox. The options in the Run and the Start At areas will become active.

10. Choose how often you want the task to run in the Run area, or select **At Startup** to run your task as soon as VirusScan 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 workstation is active and VirusScan is running. Specify in the text box provided how many minutes VirusScan 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.

11. To save your changes and return to the Automatic Update/Upgrade Properties dialog box, click **OK**. To return to the dialog box without saving your changes, click **Cancel.**

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

12. To configure additional options, click **Advanced**, then see "Configuring advanced upgrade options" to learn about your choices. To save your changes and return to the AntiVirus Console, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

Configuring advanced upgrade options

To ready your update task to run, you need to enter only a target server, a connection method, and any necessary login information. Then, once you set a schedule for it, the Automatic DAT Update utility will download the correct files from the target server for you, extract them from their .ZIP archives, and install them into the VirusScan program directory.

To do additional pre- or post-processing on the files, or to take other actions, click **Advanced** to open the Advanced Upgrade Options dialog box (Figure 8-29).

Figure 8-29. Advanced Update Options dialog box

Next, follow these steps:

1. Select the **Retrieve the Upgrade files but do not perform the upgrade** checkbox to have the utility download the .ZIP archive that contains the new upgrade files, extract them, and simply save them in a location you specify instead of installing them.

   Selecting this checkbox also selects the **Save the Upgrade files for later usage** checkbox. To tell the utility where to save the new upgrade files, enter a path and folder name in the text box provided, or click **Browse** to locate a suitable folder.

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

Updating and Upgrading from NetWare servers

If you store your .DAT files and upgrade files for retrieval from Novell NetWare servers, you must install and activate the File Copy utility included with the VirusScan program package. This utility runs automatically, without a user interface, as soon as you log in to your Windows NT workstation. Instead, it works directly with the Automatic DAT Update and Automatic Product Upgrade utilities to navigate and download files from the NetWare servers you designate in the Automatic Update/Upgrade dialog box.

To use the utility, you must install it as part of a Custom setup when you first install VirusScan. Chapter 2, Step 7 on page 35 describes the installation process.

IMPORTANT: Do *not* install the file copy utility on your system unless you use NetWare servers to distribute virus definition updates and product upgrades. If you do not have a network environment with this configuration, the file copy utility can misdirect the Automatic DAT Update and Automatic Product Upgrade utilities.

The utility also requires that you run Novell's Client32 application from the Windows NT workstation, and that you have NetWare v4.11 installed on the NetWare server.

Once installed, the File Copy utility connects to your NetWare repository, then downloads any existing .DAT files or upgrade files to a temporary directory on the local workstation. The owner of the workstation that runs the utility must have the permissions necessary to connect to the NetWare server in order for the File Copy utility to complete this operation.

When the time arrives for the scheduled update or upgrade operation to begin, the File Copy utility directs the update and upgrade utilities to retrieve the new files from the local temporary directory instead of from the NetWare server. This operation occurs without any user intervention. If the operation fails for any reason, the File Copy utility will record an error message in the VirusScan Activity Log file.

IMPORTANT: Because the File Copy utility begins to run only when you log in to your workstation, you must be sure to log in at least once in the period between your last update or upgrade operation and the next scheduled operation.

Updating .DAT files without Automatic DAT Update

Network Associates recommends that you use the Automatic DAT Update utility supplied with VirusScan in order to install new .DAT file versions. These utilities offer an easy and foolproof method for correctly updating .DAT files. If you want to install .DAT files yourself, however, you can download:

- **Regular .DAT files.** Network Associates stores these files on its FTP site as .ZIP archives with the name DAT-XXXX.ZIP. The XXXX in the file name is a series number that changes with each .DAT file release. To download these files, use a web browser or FTP client to connect with:

  ftp://ftp.nai.com/pub/antivirus/datfiles/4.x

- **Installable .EXE files.** Network Associates stores these files on its website as a self-executing setup file named XXXXUPDT.EXE. Here, too, the XXXX is a series number that changes with each new virus definition file release. To download these files, use a web browser to connect with:

  http://download.mcafee.com/updates/4x.asp

Both files contain exactly the same virus definition files. The difference between them lies in how you use them to update your VirusScan copy.

In brief, to use the DAT-XXXX.ZIP archive, you must download the file, extract it from its archive, stop the VirusScan on-access scanner, copy the files into the VirusScan program directory, then restart the VirusScan on-access scanner. See "Updating from .DAT file archives" for detailed steps.

To install .DAT files that come with their own setup utility, you need only to download the files to a temporary directory on your hard disk, then run or double-click the XXXXUPDT.EXE file. The setup utility stops the on-access scanner, copies the files to the correct directory, then restarts the on-access scanner.

IMPORTANT: Both update methods require that you have administrator rights for the workstation you want to update. You must log on to the target workstation correctly before you update your files.

Once updated, VirusScan will use the new .DAT files immediately—you do not need to restart your workstation.

Updating from .DAT file archives

To install .DAT file updates directly from a .ZIP archive WITHOUT using AutoUpdate, follow the steps below.

NOTE: Network Associates does not recommend using this method to update your .DAT files.

1. Create a temporary directory on your hard disk, then copy the .DAT file .ZIP archive you downloaded to that directory.
2. Back up or rename these existing .DAT files stored in the program directory:
   - CLEAN.DAT
   - LICENSE.DAT
   - MESSAGES.DAT
   - NAMES.DAT
   - SCAN.DAT
   - SHLDMSG.DAT

3. Use WinZip, PKUnzip, or a similar utility to open the .ZIP archive and extract the updated .DAT files.

4. Log on to the workstation you want to update. You must have Administrator rights for the target computer.

5. Click **Start**, point to **Settings**, then choose **Control Panel** to open the Control Panel window. Next, locate and double-click the Services control panel to open it.

   If the computer is running Windows NT 3.51, start Program Manager, then locate the Control Panels program group. Double-click the program group to open it, then locate and double-click the Services control panel.

6. Select the Network Associates McShield service, then click **Stop**.

7. Copy the .DAT files you extracted from the .zip archive to the VirusScan program directory. If you installed VirusScan to its default program directory, copy the files here:

   C:\Program Files\Network Associates\VirusScan NT

8. Return to the Services control panel, select the McShield Service, then click **Start**.

9. Close the Services control panel.

VirusScan will use the updated .DAT files in scan operations immediately.

Using VirusScan Administrative Utilities A

Setting user credentials for workstations

Most of VirusScan's essential functions run as Windows NT services. All of these services require a user account on the local workstation in order to obtain the rights they need to schedule and perform scan operations. Ordinarily, you set the user account that these services use when you install it on the target workstation (see Step 10 on page 37 or Step 6 through Step 9 on pages 42 to 43 for details).

If you want to have the Network Associates services switch to a different user account, however, you can do so with SVCPWD.EXE, a command-line utility that comes with the program. SVCPWD runs from the Windows NT command line and requires as input a text file that you create with a text editor, such as Notepad.

In the text file, you must list all of the computers for which you want to change the account that the services use. List each computer name in Universal Naming Convention (UNC). To change the accounts for a computer named CentAdmin and another named AVClient, for example, type these lines into a text file:

```
\\centadmin

\\avclient
```

Next, save the file in the VirusScan program directory or another convenient directory.

SVCPWD does *not* create a new account on any of the target workstations —the account you switch to must already exist on each workstation and must have administrative rights. The Network Associates services, in turn, must be set to log on as LocalSystem.

To run SVCPWD, follow these steps:

1. Click **Start**, point to **Programs**, then choose **Command Prompt**.
2. At the command prompt, change to the VirusScan program directory.
3. Type this line at the prompt:

   ```
   svcpwd <TEXTFILE.TXT>
   ```

The utility will prompt you to enter the user name for the account you want the Network Associates services to use.

4. Enter an account name, or press ENTER without entering a name to use the existing system account on the target computer. If you enter a user name, be sure to precede it with a domain name.

   For example, to use the Client account in the Mydomain domain, type `mydomain\client`, then press ENTER.

   IMPORTANT: SVCPWD will tell the Network Associates services on each of the computers you listed in the text file to use the account information you specify here. If the account does not exist on the target server, SVCPWD will stop execution.

5. If you supplied a user name for the account, the utility will prompt you to enter a password for that account as it connects with each computer listed in the text file. If you told it to use the system account, the utility will skip this step. Enter the password for the user account you want to use at the prompt, then press ENTER.

   As it contacts each listed computer, the utility will search for installed Network Associates services, then set all of them to use the account you specified.

   WARNING: Do *not* run SVCPWD during an on-demand scan operation. Doing so can interfere with the operation of the Network Associates Task Manager service.

"Broadcasting" on-demand tasks to workstations

Once you create an on-demand scan task for use on your own workstation, you can save its settings as a .VSC file, then send the task to other workstations for them to execute (see "Using VirusScan menus" on page 106 for details). Those workstation users can simply double-click the .VSC file you send to open VirusScan preloaded with the settings you saved. Although you can transfer .VSC files by nearly any normal means—as file attachments to e-mail messages, or by copying the file directly to the target system—doing so usually requires the cooperation of the other workstation owner.

VirusScan also includes another utility expressly for this purpose: you can use IMPTASK.EXE to tell the other workstation to import the task settings you saved directly from your own computer. IMPTASK runs from the Windows NT command line and requires as input a .VSC file that you create from the VirusScan stand-alone on-demand scanner.

To run SVCPWD, follow these steps:

1. Click **Start**, point to **Programs**, then choose **Command Prompt**.
2. At the command prompt, change to the VirusScan program directory.
3. Type this line at the prompt:

   ```
   imptask /file <SETTINGS.VSC>
   ```

   This tells the copy of VirusScan on your local workstation to import the settings in the file SETTINGS.VSC, or from whichever .VSC file you designate.

   To tell a different computer elsewhere on the network to import the same settings file, type this line at the prompt instead:

   ```
   imptask /file <SETTINGS.VSC> /server \\<COMPUTERNAME>
   ```

   Adding the option /SERVER tells IMPTASK to copy the settings file to any computer you designate on the same line with Universal Naming Convention.

Network Associates Support Services

B

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 four levels of extended support under the Network Associates Corporate PrimeSupport program. If you purchased a retail version of a Network Associates product, you can choose a plan geared toward your needs from the Retail PrimeSupport program.

PrimeSupport Options for Corporate Customers

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

PrimeSupport KnowledgeCenter

PrimeSupport KnowledgeCenter gives you access to technical support assistance via a Network Associates online knowledge base, in addition to product upgrades via the Network Associates website. If you purchased your Network Associates product with a subscription license, you receive PrimeSupport KnowledgeCenter as part of the package for either one or two years from your date of purchase, depending on the length of your subscription. If you purchased your Network Associates product with a one-year license, you can renew your PrimeSupport KnowledgeCenter plan for an annual fee.

To receive your KnowledgeCenter password or to register your PrimeSupport agreement with Network Associates, visit:

http://knowledge.nai.com/

Your completed form will go to the Network Associates Customer Care Center. You must complete this form before you connect to the PrimeSupport KnowledgeCenter or before you call Network Associates PrimeSupport.

PrimeSupport KnowledgeCenter features:

- Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes
- Unrestricted, 24-hour-per-day access to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website

PrimeSupport Connect

PrimeSupport Connect gives you telephone access to essential product assistance from experienced Network Associates technical support staff members.

PrimeSupport Connect features:

- Unlimited toll-free telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time
- Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes
- Unrestricted, 24-hour-per-day access to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website

PrimeSupport Connect 24-By-7

PrimeSupport Connect 24-By-7 gives you round-the-clock telephone access to essential product assistance from experienced Network Associates technical support staff members. You can purchase PrimeSupport Connect 24-By-7 on an annual basis when you purchase a Network Associates product, either with a subscription license or a one-year license.

PrimeSupport Connect 24-By-7 features:

- Unlimited toll-free telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time
- Priority call handling during business hours
- After-hours responses for urgent issues within one hour, including weekends and local holidays
- Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes
- Unrestricted, 24-hour-per-day access to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website

PrimeSupport Enterprise

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

PrimeSupport Enterprise features:

- Unlimited, toll-free telephone access to an assigned technical support engineer on a 24-hour-per-day, seven-day-per-week basis, including on weekends and local holidays
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times from your support engineer, who will respond to pages within half an hour, to voice mail within one hour, and to e-mail within four hours

- Ability to designate at least five people in your organization as customer contacts
- The option to be a beta site for new Network Associates products
- Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes
- Unrestricted, 24-hour-per-day access to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website

Ordering Corporate PrimeSupport

To order PrimeSupport KnowledgeCenter, PrimeSupport Connect, PrimeSupport Connect 24-By-7, or PrimeSupport Enterprise for your Network Associates products:

- Contact your sales representative; or
- In North America, call Network Associates Support Services at (800) 988-5737 or (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.

Table B-1. Corporate PrimeSupport at a Glance

Feature	Knowledge Center	Connect	Connect 24-By-7	Enterprise
Technical support via website	Yes	Yes	Yes	Yes
Software updates	Yes	Yes	Yes	Yes
Technical support via telephone	—	Monday–Friday 8:00 am–8:00 pm Central Time	Monday–Friday 8:00 am–8:00 pm Central Time After-hours emergency response	24-hour-per-day access to your assigned support engineer (24 hours per day, 7 days per week)
Priority call handling	—	—	Yes	Yes
After hours support	—	—	Yes	Yes
Assigned support engineer	—	—	—	Yes
Proactive support contact	—	—	—	Yes
Designated customer contacts	—	—	—	At least 5
Committed response time	—	—	Within 1 hour for urgent issues	After hours pager: 30 minutes Voicemail: 1 hour E-mail: 4 hours

PrimeSupport Options 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 (see the chapter or appendix about software updating in your anti-virus software *User's Guide* for details). 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 (see the chapter or appendix about software updating in your anti-virus software *User's Guide* for details). 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 24-hour-per-day, seven-days-per-week access to online or electronic support through the Network Associates voice and fax system, the Network Associates website, and through such other electronic services as America Online and CompuServe.

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

  – Automated voice and fax system: (408) 346-3414

  – Network Associates website: http://support.nai.com

  – CompuServe: GO NAI

  – America Online: keyword MCAFEE

- Free access to the PrimeSupport KnowledgeBase: online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes. Visit the KnowledgeBase at:

  http://knowledge.nai.com

- 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.

You can also take advantage of a variety of additional support options geared toward your needs. You can purchase these options either with your Network Associates product or after your complimentary 90-day support period expires:

- **Small Office/Home Office Annual Plan.** This plan gives you unlimited toll-free access to technical support during regular business hours, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time.
- **Pay-Per-Minute Plan.** This plan gives you support only when you need it: 900-number access to technical support features priority call handling to minimize your hold time and the first two minutes of support free.
- **Online Upgrades Plan.** This plan gives you the convenience of automatic access to product upgrades via Network Associates online or electronic services.
- **Quarterly Disk/CD Plan.** This plan gives you automatic quarterly delivery of upgrade disks or CDs if you cannot access product upgrades online. This service is available for VirusScan and NetShield only.

Ordering Retail PrimeSupport

To order the PrimeSupport Small Office/Home Office Annual Plan, Pay-Per-Minute Plan, Online Upgrades Plan, or Quarterly Disk/CD Plan for your Network Associates products:

- In North America, call Network Associates Customer Care at (972) 278-6100; or
- Visit the Network Associates website at:

  http://www.nai.com/services/support/add_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 Global Professional 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.

Jumpstart Services

You can take advantage of a variety of Jumpstart Services to help you implement your new Network Associates product:

- **Basic and Advanced.** This service installs, configures, and optimizes your new Network Associates product, and gives basic operational product knowledge to your team.
- **Selfstart.** This service helps prepare you to perform your new product implementation on your own and, in some cases, installs the product.
- **Proposal Development.** This service evaluates processes and procedures as well as hardware and software requirements prior to a new product implementation, enabling a consultant to prepare your custom proposal.

Network Consulting

Network Associates consultants provide expertise in protocol analysis and a vendor-independent perspective that creates unbiased solutions for troubleshooting and optimizing your network. Also, their broad understanding of network management best practices and industry relationships speeds escalation of problems through vendor support.

You can order a custom consultation to help with planning, design, implementation, and ongoing management of your network. With it, you can assess the impact of rolling out new applications, network operating systems, or internetworking devices.

Contact Network Associates Consulting Services at 1-800-395-3151 to learn more about the options available, or visit the Network Associates website at:

http://www.nai.com/services/consulting/consulting.asp

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.

Contact your sales representative to learn more about these programs, or call Network Associates Total Education Services at 1-800-395-3151. You can also visit the Network Associates website at:

http://www.nai.com/services/education/

Using SecureCast to Obtain New Data Files

C

Introducing SecureCast

The Network Associates SecureCast service provides a convenient method you can use to receive the latest data (.DAT) file updates automatically, as they become available.

To use this option, both retail and corporate users must install BackWeb client software. Next, retail customers must subscribe to the SecureCast Home channel (also called SecureCast VirusScan channel). Corporate customers must subscribe to the Enterprise SecureCast channel.

NOTE: If you are a corporate customer, you must first have a grant number (product serial number) to subscribe to Enterprise SecureCast.

If you do not have a grant number, please contact your purchasing agent, your Value Added Reseller, or Network Associates Customer Care at (408) 988-3832 for assistance.

If you are already a registered Network Associates customer and do not know your grant number, submit the grant-number request form online:

http://www.nai.com/products/securecast/esc/grantreq.asp

OR

Send an e-mail message to the appropriate address:

ESCRegistration@nai.com (United States)

ESC-Registration-Europe@nai.com (Europe)

ESC-Registration-Asia@nai.com (Asia)

Whether you are a retail client or a corporate client, BackWeb provides a variety of options to tailor the way BackWeb relates to the SecureCast channel. Online help for configuring BackWeb is available at:

http://www.backweb.com/doc/version30/Client/

NOTE: If you are a corporate customer, but not the network administrator, contact your administrator to learn where to update your files, or use VirusScan's Automatic DAT Update feature. See "Configuring Automatic DAT Update options" on page 145 for more information.

Why should I update my data files?

Your software relies on information in its virus definition files (.DAT) files to identify viruses. More than 200 new viruses appear each month, however, and older .DAT files may not recognize them. To meet this challenge, Network Associates releases new .DAT files every four to six weeks. You are entitled to these free data file updates for use with your version of the software. If you do not use current .DAT files you may compromise your virus-protection program. Network Associates strongly recommends that you update your .DAT files on a regular basis.

IMPORTANT: Using current virus identification files is only one element of an effective virus protection program. It is equally important to use a scanning engine that incorporates current advances in virus detection and cleaning. Periodically, Network Associates releases an upgrade of its scan engine that incorporates these advances.

Earlier .DAT files, however, may not function properly with newer scan engines. When the older scan engine becomes obsolete, Network Associates will discontinue development of .DAT files for it. You should upgrade your software before your current version becomes obsolete.

Which data files does SecureCast deliver?

With SecureCast, you'll receive automatic downloads of these common data files:

- NAMES.DAT—includes virus names and other details that the user sees when viewing the Virus List.
- SCAN.DAT—includes detection string data for all viruses detected.
- CLEAN.DAT—includes removal string data for all viruses cleaned.

In addition to these common .DAT files you may receive some additional files, depending on which anti-virus or security products you use:

- WEBSCANX.DAT or INTERNET.DAT—includes detection string data for hostile Java applets and ActiveX controls. WebShieldX and VirusScan use these files.
- MCALYZE.DAT—includes detection string data for complex polymorphic virus detection. Network Associates 32-bit products with engine versions 3.0.0 through 3.1.4 use this file.
- POLYSCAN.DAT—includes detection string data for complex polymorphic virus detection. Network Associates 32-bit products with engine versions 3.1.5 and later use this file.

System requirements

- Windows 95 or later, or Windows NT.
- At least 100MB free hard disk space: Home SecureCast (client and channel) 7MB, plus 3–6MB per download. Enterprise SecureCast (client and channel) 15MB, plus 6–6.5MB per download.
- An active Internet connection—direct or dial-up—for a minimum of one hour per week.

SecureCast features

- SecureCast uses client software developed with BackWeb Technologies.
- SecureCast eliminates the need for downloading update files from Network Associates electronic services.
- SecureCast works invisibly in the background, allowing other applications to take priority over it, using your Internet connection when it's idle. However, you can configure your desktop client so that SecureCast downloads have a higher priority.
- SecureCast works with most corporate firewalls.
- SecureCast supports 32-bit TCP/IP connections for Enterprise SecureCast and Home SecureCast channel subscribers, and provides non-Internet connections for retail customers using asynchronous modem dialup.
- SecureCast delivers .ZIP, .EXE, and .DAT files to your desktop as BackWeb InfoPaks.

Free services

- Automatic delivery of .DAT files, usually available mid-month.
- Alerts on newly identified dangerous viruses.
- Announcements of new versions of software and associated products.

VirusScan SecureCast Channel

SecureCast can be installed from many Network Associates CD-ROMs. If your software does not include SecureCast, you can download it from the Web.

- if you are a retail user, go to:

  http://download.mcafee.com/securecast/scast.asp

- if you are a corporate user, go to:

  http://www.nai.com/products/securecast/esc/default.asp

Installing BackWeb Client and SecureCast

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

- Download and install BackWeb (Step 1 to Step 12).
- Configure BackWeb (Step 13 to Step 19).
- Register to receive SecureCast InfoPaks via BackWeb (Step 20 to Step 29).

Phase 1: Download and install BackWeb

1. Select SecureCast from the choices on the installation CD-ROM, or locate the file that you downloaded from the Web and double-click its icon:
   - The retail version is named VS_BWClient.EXE.
   - The corporate version is named ESC_BWClient.EXE.
2. A dialog box appears advising you that you are about to install BackWeb (Figure C-1).

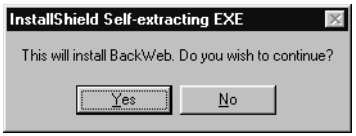


Figure C-1. InstallShield Self-extracting file dialog box

Click **Yes** to proceed with the installation. The Install Shield Self-extracting EXE progress window appears (Figure C-2).

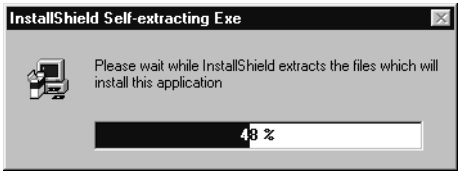


Figure C-2. InstallShield Self-extracting Exe progress window

As soon as the necessary installation files have been extracted, the InstallShield **Welcome** panel for BackWeb appears (Figure C-3 on page 177).

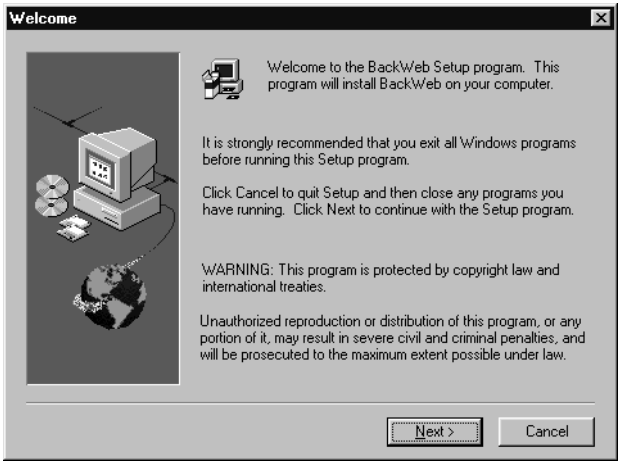


Figure C-3. InstallShield Welcome panel

3. Read the instructions and warnings on this panel. Then click **Next**. The BackWeb license agreement appears (Figure C-4).

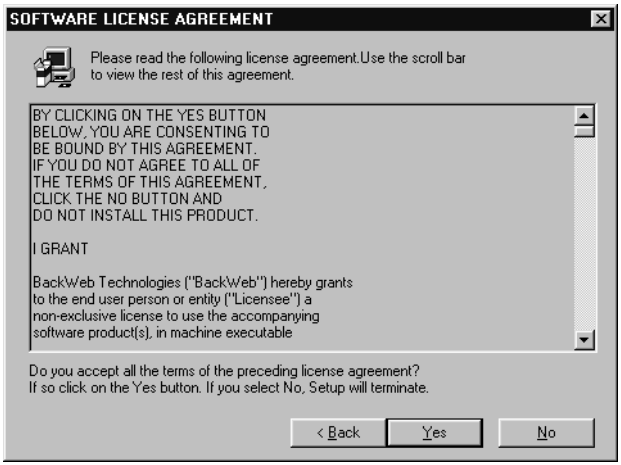


Figure C-4. BackWeb Software License Agreement panel

If you agree to abide by the terms and conditions of the license agreement, click **Yes** to continue. The **Choose Destination Location** panel appears (Figure C-5 on page 178).

Figure C-5. BackWeb Destination Directory panel

4. Review the location where the program will be installed. Click **Next** to accept the default location, or click **Browse** to select a different location for the program files. After you select an alternative destination directory you are returned to the **Choose Destination Location** panel. If you are satisfied with your selection of destination, click **Next**. InstallShield displays a BackWeb installation-progress meter (Figure C-6).

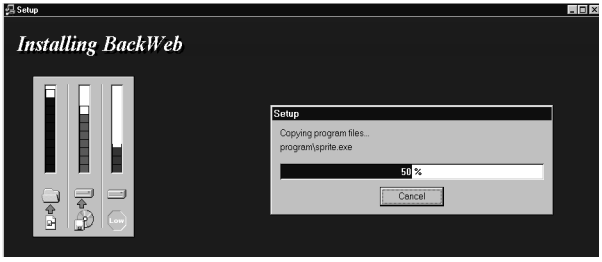


Figure C-6. BackWeb Setup Progress window

When the installation is complete, the InstallShield **Connection Type** panel appears (Figure C-7 on page 179).

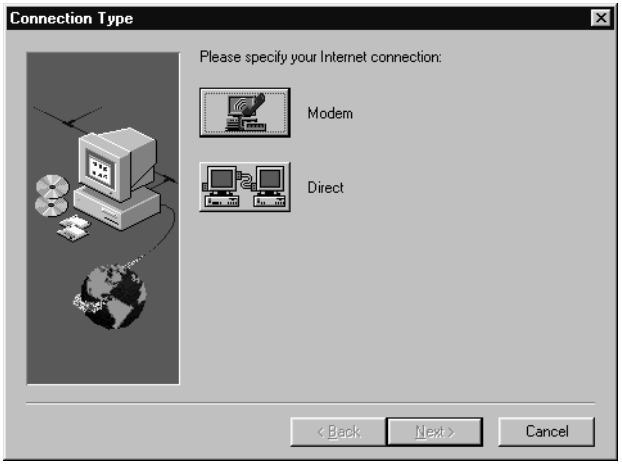


Figure C-7. InstallShield Connection Type panel

5. Click either the **Modem** or **Direct** (that is, a LAN connection) button to specify the type of Internet connection you use.

   - If you select **Modem**, proceed to Step 10.
   - If you select **Direct**, the **Communication Method** panel appears (Figure C-8). Proceed to Step 6.

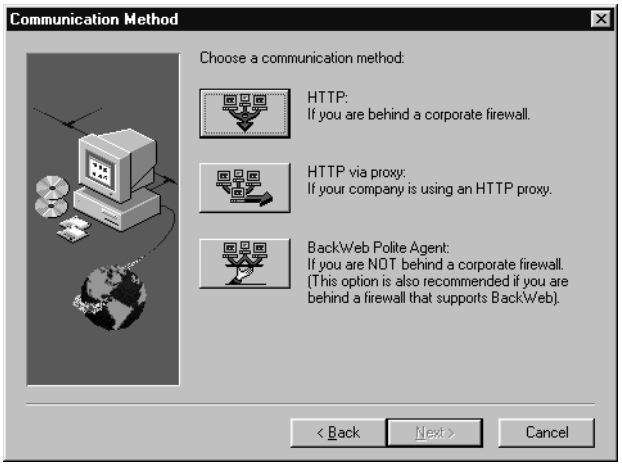


Figure C-8. InstallShield Communication Method panel

6. Click the button that represents the way that your computer communicates with the Internet.
   - If you select **HTTP**, (that is, your company does not use a proxy server when connecting to the Internet, proceed to Step 10.
   - If you select **HTTP via proxy**, proceed to Step 7.
   - If you select **BackWeb Polite Agent**, proceed to Step 10.

NOTE: The BackWeb Polite agent allows you to control the way BackWeb relates to other applications that may be running when InfoPaks arrive at your desktop. For more information see the BackWeb on-line help at:

http://www.backweb.com/doc/version30/Client/

In particular, see Application Politeness, under Customizing BackWeb, in the Getting Started section.

---

7. If you selected **HTTP via proxy**, the **HTTP Proxy Setup** panel appears (Figure C-9).

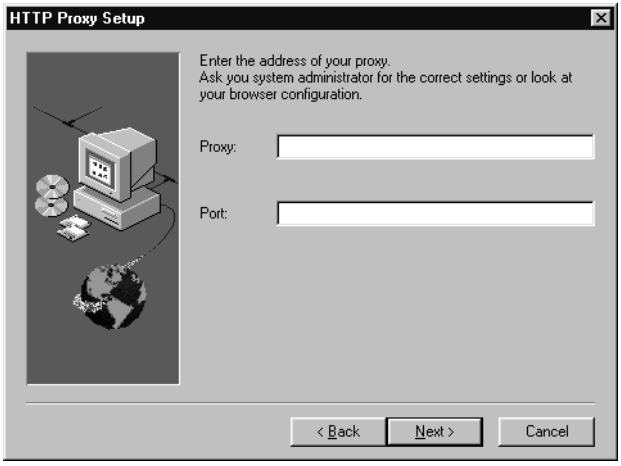


Figure C-9. InstallShield HTTP Proxy Setup panel

8. Enter the Proxy identification and the Port it uses. Then click **Next.** The **Proxy Authentication** panel appears (Figure C-10 on page 181).

Figure C-10. InstallShield Proxy Authentication panel

9. If the Proxy server requires authentication of user identification, enter the username and password that will permit access. Then, click **Next**.

10. The InstallShield **Setup Complete** panel appears (Figure C-11).

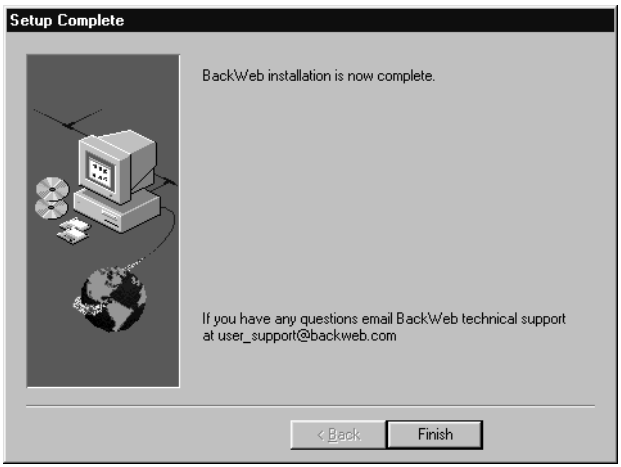


Figure C-11. InstallShield Setup Complete panel

11. Click **Finish** to complete the first phase of the installation and setup process. A message appears indicating that BackWeb is ready to receive InfoPaks (Figure C-12). These are the information packets, including updated .DAT files, new viruses alerts, and other important messages from Network Associates. .

Figure C-12. BackWeb Installation Complete message

NOTE: The message shown here appears during installation of SecureCast for use with Network Associates retail products. A slightly different message appears during installation of SecureCast; for use with software that is licensed for use in corporate environments.

12. Click **OK** and move to phase two of the SecureCast set-up process.

Phase 2: Configure BackWeb

13. The **BackWeb Quick Setup Welcome** panel appears (Figure C-13).

Figure C-13. BackWeb Quick Setup Welcome panel

14. Click **Next**. The **BackWeb InfoPaks** panel appears (Figure C-14).

Figure C-14. BackWeb Quick Setup InfoPaks panel

15. Click **Sample Flash** for a demonstration of InfoPak messaging styles. When you have finished viewing the demonstration, click **Next**. The **BackWeb Auto-player** panel appears (Figure C-15).

Figure C-15. BackWeb Quick Setup Auto-player panel

16. Select the types of InfoPak messaging you want BackWeb to display. The types available are: **BackWeb Flashes**, **Screen Savers**, **Wallpaper** and **Audio Messages**. After making your choice(s), click **Next**. The **BackWeb Channels** panel appears (Figure C-16 on page 184).

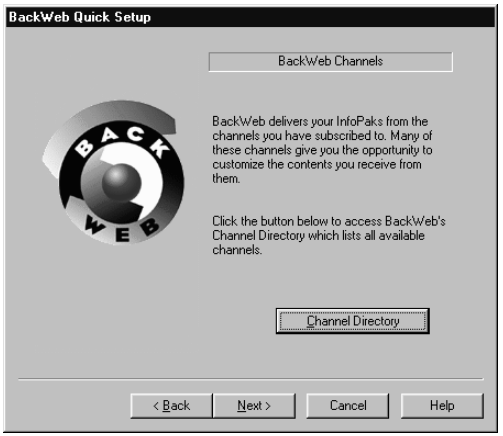


Figure C-16. BackWeb Quick Setup Channels panel

17. Click **Channel Directory** if you want to subscribe to additional BackWeb channels in addition to SecureCast. When you have finished, click **Next**. The **BackWeb Disk Space** panel appears (Figure C-17).

Figure C-17. BackWeb Disk Space panel

18. Use the buttons to specify the amount of hard disk space on your computer that you want to allocate to the InfoPaks that BackWeb delivers. When you have finished, click **Next**. The **BackWeb Successful Completion** panel appears (Figure C-18 on page 185).

Figure C-18. BackWeb Successful Completion panel

19. Click **Finish** to move to phase three of the SecureCast set-up process.

Phase 3: Register to receive SecureCast InfoPaks via BackWeb.

20. The BackWeb interface is now fully visible (Figure C-19). The first InfoPak that BackWeb will deliver is the SecureCast registration form(s).

IMPORTANT: If you are a corporate user, and have a high-speed Internet connection, the window may list **Register Now** as an already received InfoPak. Continue with Step 21.

If you use a retail product, have a slower connection, or if there is unusually heavy traffic at the SecureCast site or your site, the window may list no InfoPaks. In that case, minimize or close the BackWeb window. After some time, you will receive a Flash message. Click in the flashing message and continue with Step 22.

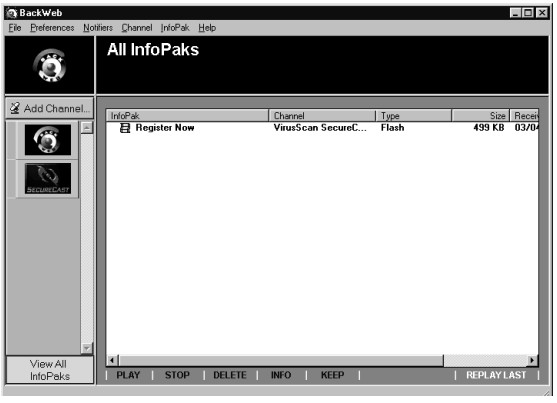


Figure C-19. BackWeb User Interface

21. When **Register Now** is listed in the window, double-click it. The SecureCast Flash banner appears (Figure C-20).

Figure C-20. SecureCast Flash banner

22. Click in the banner. The **Network Associates Welcome** panel appears (Figure C-21).

Figure C-21. Network Associates Welcome panel

23. Review the information. Then click **Register Now** at the bottom of the panel. The **Inbox** folder that BackWeb created during the installation process appears, containing the **BWRegister . . .**icon (Figure C-22).

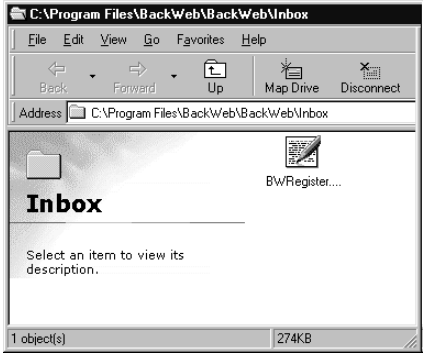
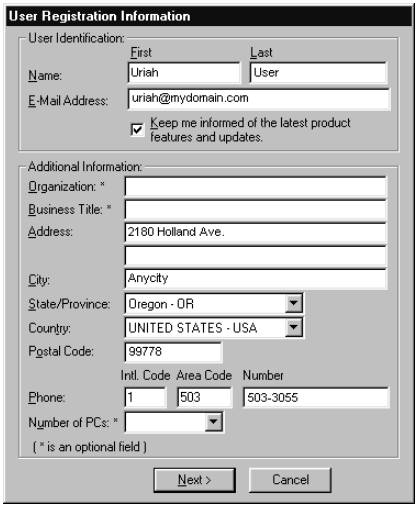
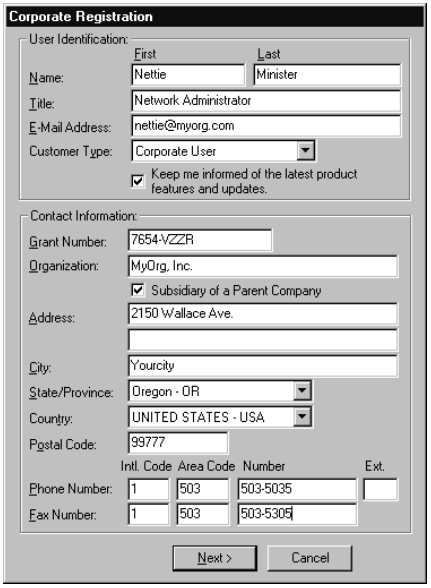


Figure C-22. BackWeb Inbox folder

24. Double-click the **BW Register . . .** icon. A registration information form appears. The form for retail users is different from the form for corporate users (Figure C-23).



Retail User Registration form



Corporate User Registration form

Figure C-23. SecureCast User Registration Information form

25. Provide the information required. When you have finished, click **Next**.

> **NOTE:** If you are a corporate user, and your company is not a subsidiary of another company, clear the **Subsidiary of a Parent Company** checkbox before proceeding.

- If you have not cleared the **Subsidiary of a Parent Company** checkbox, the **Parent Company Information** dialog box appears (Figure C-24 on page 188). Proceed to Step 26.
- If you have cleared the **Subsidiary of a Parent Company** checkbox, proceed to Step 27.

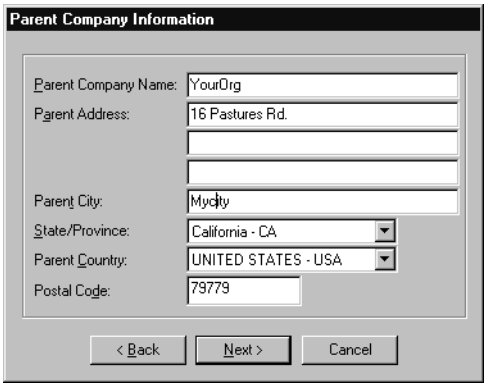


Figure C-24. SecureCast Parent Company Information form

26. If your company is the subsidiary of another company, your are asked to provide information about the parent company. When you have finished, click **Next**. The **Proxy Communication Configuration** dialog box appears (Figure C-25).

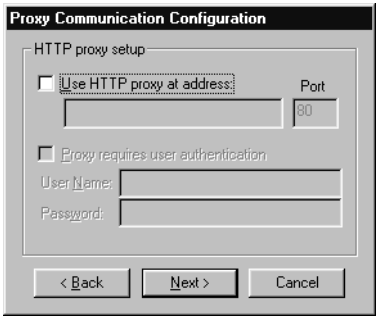


Figure C-25. SecureCast Proxy Communication Configuration

27. If you use an HTTP proxy, provide the information required:
    - Select **Use HTTP proxy at address** checkbox.
    - Enter the address of the HTTP proxy and confirm that the correct Port is displayed.
    - Select **Proxy requires users authentication** if appropriate, and enter your user name and password.

28. When you have finished, click **Next**. The **Online Activity Status** panel appears displaying the progress of the registration process (Figure C-26 on page 189).

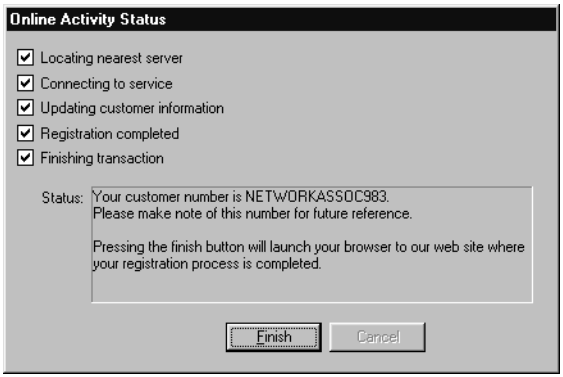


Figure C-26. SecureCast Online Activity Status panel

29. Click **Finish** after a checkmark appears in all the boxes. The set-up process in complete. Your web browser will open to the Network Associates SecureCast electronic customer care page. If you are a corporate user, the window resembles the one shown in Figure C-27:

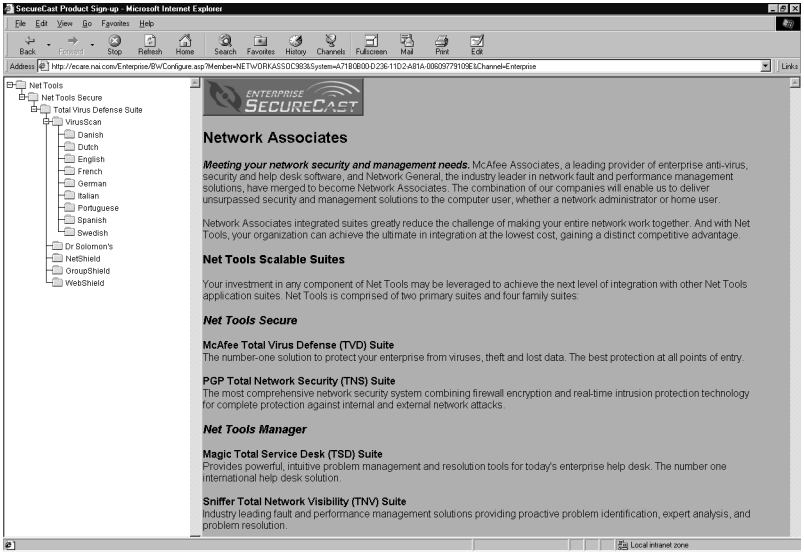


Figure C-27. SecureCast Electronic Corporate Customer Care

If you use a retail product, the window resembles the one shown in Figure C-28 on page 190.

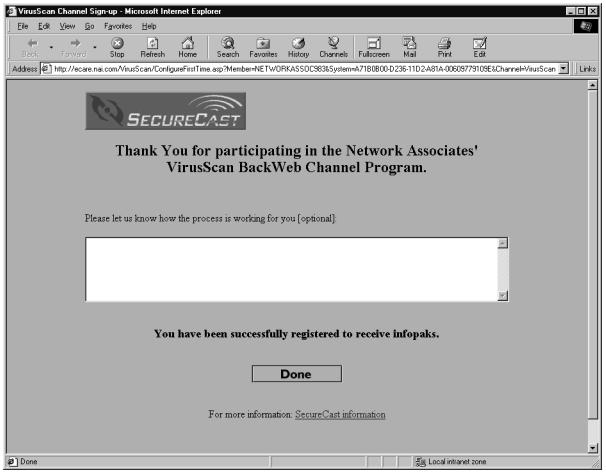


Figure C-28. SecureCast Electronic Retail Customer Care

Troubleshooting Enterprise SecureCast

Registration problems

If you try to register during a busy time of day on the web, you may encounter a delay while the server tries to process your registration request. If you receive the error message "1105 Error" or "Database Error: Unable to connect to the data source," this means that there is a database problem on the SecureCast server. Try submitting the form again, or try to register later. If you continue to have problems subscribing to the Enterprise SecureCast channel, please contact Network Associates Download Support (Monday to Friday, 8 A.M. to 8 P.M. Central time) at (972) 278-6100.

Unsubscribing from SecureCast

Follow these steps to cancel this service at any time:

1. In the list box on the left side of the BackWeb interface, select the SecureCast service to which you have subscribed (Enterprise SecureCast or VirusScan SecureCast).
2. Right-click and select **Unsubscribe**. All InfoPaks listed in the SecureCast window will be deleted and you will no longer receive them.

Support Resources

SecureCast

If you have additional questions about SecureCast, consult the SecureCast FAQ:

http://www.nai.com/products/securecast/esc/enterprise_faq.asp

BackWeb

- For a general description of BackWeb and InfoPaks, read the BackWeb Overview:

  http://www.nai.com/products/securecast/anchor.asp

- For a comprehensive guide to BackWeb (including additional troubleshooting advice), bookmark the BackWeb User's Manual:

  http://www.backweb.com/doc/version30/

- For solutions to serious problems with the operation of BackWeb, please contact Network Associates Download Support (Monday to Friday, 8 A.M. to 8 P.M. Central Time) at (972) 278-6100.

Index

A

B

C

D

E

F

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Z