User’s Guide

NetShield for Windows NT

2805 Bowers Avenue
Santa Clara, CA 95051-0963

Phone:(408) 988-3832
Monday - Friday
6:00 A.M. - 6:00 P.M.

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 obligations whatsoever. Please address your feedback to: Network Associates, Inc., Documentation, 2805 Bowers Avenue, Santa Clara, CA 95051-0963, send e-mail to documentation@cc.nai.com, or send a fax to Network Associates Documentation at (408) 970-9727.

Issued January 1998/NetShield for Windows NT v3.1.4

Table of Contents

Preface viii

Chapter 1. Introducing NetShield 12

Introduction 12

What Is NetShield? 13

NetShield Features 14

Superior detection 14

Automated protection 14

Administrative ease 14

How To Contact Network Associates 16

Customer service 16

Technical support 16

Network Associates training 17

International contact information 18

Reporting new viruses for NetShield updates 19

Chapter 2. Installing NetShield 21

Overview 21

Before You Start 22

System requirements 22

Performing a Local Installation 24

Performing a Remote Installation 26

Performing a silent installation 28

Customizing the silent installation 28

Chapter 3. Getting Started 32

Launching the AntiVirus Console 32

Remote Administration 34

Chapter 4. Using the AntiVirus Console.....35

What Is a Task? 35

Working with Tasks 36

Using the Statistics window 36

Importing and exporting tasks..... 36

Copying and pasting tasks..... 38

Disabling tasks..... 39

Deleting tasks 39

Chapter 5. On-access Scanning.....40

The On-access Task 40

Viewing on-access status 40

Editing the on-access task..... 41

Chapter 6. On-demand Scanning.....53

On-demand Tasks..... 53

Creating an on-demand task..... 53

Editing an on-demand task 54

Chapter 7. Virus Notification 68

Using Alert Manager 69

Viewing the Summary page 71

Forwarding alerts to another computer 72

Sending a network message..... 75

Sending a SMTP alert to an e-mail address 78

Sending an alert to a pager..... 81

Sending an alert to a printer..... 85

Using SNMP services 88

Using DMI alerting 90

Executing a program on alert..... 92

Using audible alerting 94

Logging with Alert Manager 96

Using Centralized Alerting 99

How Centralized Alerting works..... 99

Configuring Centralized Alerting 99
Customizing Alerts 100
Enabling/disabling alerts 100
Changing the priority of an alert 101
Customizing an alert message 102

Chapter 8. Updating NetShield 103

Overview 103
Using AutoUpdate 104
Automatic .DAT Update task 105
Automatic Product Upgrade task 109
Scheduling AutoUpdate tasks 114
Updating your .DAT files manually 115
Validating the NetShield program files 116

Appendix A. Encountering Viruses 117

Removing Viruses 117
If you selected Clean Infected Files 118
If you selected Delete Infected Files 118
If you selected Move Infected Files 119
If you selected Continue Scanning 119

Appendix B. Using VirusScan 120

What is VirusScan? 120
Using VirusScan 121
Configuring scan options 121
Responding to infections 122
Reporting options 123

Appendix C. Network Associates Support Services 125

Customer Service Programs 126
Free 90-day introductory support program 126
Subscription maintenance and support program 127
Optional support plans 128

Professional Services Programs 129
Training 129
Consulting 129
Jump Start program 130
Enterprise support 130
Optional enterprise support feature 131

Appendix D. Updating Your Software Using SecureCast 133

Introducing SecureCast 133
Why would I need to update my data files? 134
Which data files does SecureCast deliver? 134
System requirements 135
SecureCast features 135
Free services 135

Home SecureCast Channel 136
Understanding SecureCast 136
Downloading automatically 136
Unsubscribing from Home SecureCast 137

Initiating a Download 138
Updating registered software 138
Registering evaluation software 146

Enterprise SecureCast Channel 150
Benefits 150
Setting up Enterprise SecureCast 151
Using Enterprise SecureCast 152
Troubleshooting Enterprise SecureCast 153
Unsubscribing from Enterprise SecureCast 154

Support Resources 155
SecureCast 155
BackWeb 155

Appendix E. Additional Command-line Utilities 156

Using the Service Password utility 156

Using the IMPTASK utility 158

Appendix F. Reference 159

VirusScan Command-line Options 159

Scan command option examples 175

VSC File Format 177

ScanOptions 177

AlertOptions 179

ActivityLogOptions 180

TaskDefinition 182

Scheduler 183

Centralized Alerting .ALR File Format 184

Index 186

Preface

The Bits and the Bytes

Computer viruses, most users know, can have a devastating impact on productivity. What many of those same users don't know is basic information that could help them protect themselves from infection—such as where viruses come from and how they operate.

In the beginning

The conceptual foundations for viruses have been around much longer than the virus threat itself. Although virus historians disagree on the specific whens and wheres, it is generally accepted that the ideas were born when computers were still huge and expensive—the domain of large corporations and the government, not the public. And while many of the viruses circulating today are malicious, destruction of data was not part of the original premise.

The idea was that if one could create a computer program that could make copies of itself, or self-replicate, it might also be possible for that program to evolve. If an error were to occur in the replication process, the resulting code (the bits of information that make up the program) would be mutant. Just as mutant genetic code is what disposes a biological virus to either be more or less able to survive and propagate, mutant digital code might dispose a computer virus to be more or less able to survive in the computer environment. Given enough time, the logical extension of the theory goes, a computer virus could evolve into something approaching artificial intelligence. Science fiction suddenly starts to look more like science and less like fiction.

What viruses really are

At its core, a virus is simply a program with one goal: self-replication. Part of achieving that goal is remaining undetected. If a virus is found by a user, it is likely to get deleted, which puts quite a damper on any self-replicating plans. Just like any other program, a virus has to be run to do its work. And since a user will not run a virus intentionally, the virus has to attach itself to a file that the user will run. That includes executable files and document files with embedded macros, as we will see in a couple of pages. For a virus to infect any other type of file—say, a plain text file—would be counter-productive: Remember, replication is its primary objective.

Computers with the sniffles?

Consider the similarities between computer and biological viruses. A computer virus infects a host program, just as a biological virus infects a host cell. It writes its own code in among the pieces of code that make up the host program. Then, in much the same way as a biological virus uses resources from its host organism to reproduce, a computer virus runs each time the infected host is run, and makes copies of itself. Those copies then infect other programs, and the cycle begins again.

Just as biological viruses have detrimental effects, so do their computer counterparts. The first computer viruses were simply experiments by research scientists to test the theory—to see if it could be done. They proved the theory, but also discovered that viruses had some unfortunate side effects. Viruses got in the way of some of the normal processes of the computer and caused erratic behavior. Many viruses are now specifically programmed to perform some function outside of self-replication. This function, called the payload, can be as innocuous as displaying a message on the computer's monitor or as harmful as destroying data on the system's hard disks. It is delivered when the trigger, an event such as a particular combination of keystrokes, a certain date or a pre-determined number of actions, occurs.

Who writes viruses?

The reason for this change in the behavior of viruses—from innocent experiment to malicious sneak attack—is a result of a change in the type of people who write them. Virus code is now developed by many people who are less interested in studying the possibility of artificial intelligence than in inflicting harm. Some do it out of spite, some because they aspire to be the underground "mad hacker" romanticized in much of pop culture as a freedom fighter of the digital age. The reasons people write virus code are probably as varied and strange as the reasons people perform other destructive acts.

Some virus writers actually choose to identify themselves, such as the Pakistani brothers who wrote the Brain virus. The brothers included the name, address, and telephone number of their software company in the viral code. When the payload was delivered, this information would be displayed for the user. Apparently, the brothers wrote the virus to show how widespread software pirating was. They put it on diskettes leaving their office with the idea that wherever the virus spread, so had their software. Of course, what they overlooked was the fact that the virus spread by infecting programs other than the one it left their office in.

Other virus writers are disgruntled employees seeking revenge. Still others are schoolkids who write just to see if they can. The famous Stoned virus is said to have been written by such a youngster. Having written it, he feared the consequences of unleashing it, so he destroyed all copies of the virus except one, which he kept at his house. His younger brother and a couple of friends managed to lay their hands on it though, and infected some disks as a joke. But the infection spread quickly and soon was impossible to stop.

Whatever the motivation, the number of people capable of writing a virus is growing right alongside the computer industry. Those who stand to be affected by virus infection—anyone who uses a computer—should be alert and wary.

Only getting worse

In part, the fact that there are so many of us who need to be on the alert today is what makes virus proliferation possible. When the computer world was made up entirely of huge expensive machines, a virus did not have very far to go once it got started. But with the advent of the personal computer, viruses suddenly had a lot of places to go. The rapid growth of the Internet, the capability to attach files to e-mail messages, and the increasing degree to which the world depends on its computers all make conditions ever-better for the spread of computer viruses.

New developments

There are other reasons to be especially wary these days. Viruses get increasingly complex and advanced as computers on the whole do the same. Just in the last few years, sophisticated and dangerous new virus families have appeared, such as polymorphic viruses and macro viruses. Polymorphic viruses are especially tricky because they change each time they infect a new file. Where once anti-virus software could search for viruses by "signatures" (chunks of code unique to each virus), software must now be able to detect polymorphic viruses that change their signature each time they infect a file.

Macro viruses infect documents and document templates—new territory for viruses. Documents used to be safe from viral attack because until a few years ago, a document file didn't have any executable code in it. Now that software applications like Microsoft Word and Microsoft Excel have embedded macro capabilities, viruses can infect documents created by that software through the macro language.

All that just in the last few years. And viruses as a serious threat have only been around for about ten years. To imagine what is in store as the computer becomes more complicated and more a part of everyday life is frightening. Luckily, you have purchased the best protection against infection available today. And with Network Associates' outstanding support and worldwide anti-virus research teams, you can make sure your protection keeps up with the ever-changing computer world.

1 Introducing NetShield

Introduction

Networked computing and the emergence of collaborative technologies have dramatically increased the speed at which viruses spread in the corporate workplace. According to a recent Virus Prevalence Survey by the NCSA, over 99.3% of corporate networks had a virus outbreak within the last year.

Infected files in a network environment can rapidly escalate an individual user incident into a large-scale virus outbreak. The expense of cleaning a network-based infection can be staggering. These expenses include: lost employee productivity, potential loss of data, internal help desk service costs, and additional network administrator and desktop service personnel support. These issues make server virus protection a must and during critical business cycles, could cost your company its edge.

What Is NetShield?

NetShield is a superior client/server anti-virus solution. NetShield combines Network Associates' award-winning Hunter virus scanning technology with robust server management capabilities to minimize the virus threat within networks. Hunter scanning technology combines several virus analysis technologies to detect all virus types, including Word and Excel macro, boot sector, file, multi-partite, stealth, polymorphic, and encrypted viruses. The Hunter engine also stops viruses written in Visual Basic 5.0, Office 95, and Office 97 file formats, ensuring protection against the newest threats to data security.

NetShield is an important element of a comprehensive security program that includes regular backups, meaningful password protection, training, and awareness. Network Associates urges you to set up and comply with such a security program to prevent future infection. For tips on creating a secure environment, see Appendix A, "Preventing Virus Infection."

NetShield Features

Superior detection

- NCSA-certified, NetShield's scanner ensures detection of 100% of the viruses found "in the wild." Visit the NCSA website (www.ncsa.com) for certification status.
- NetShield's Hunter scan technology identifies viruses with pinpoint accuracy.
- On-access (inbound and outbound) scanning provides real-time identification of both known and unknown viruses upon file access, create, copy, rename, and run; disk access; system startup; and system shutdown.
- On-demand scanning provides for user-initiated detection of known boot, file, macro, multi-partite, stealth, encrypted, and polymorphic viruses located within files, drives (local and network), and diskettes.
- NetShield scans and cleans compressed files.
- NetShield detects unknown macro viruses by using heuristic scanning technology.

Automated protection

- NetShield can be configured for an automated response on virus detection including notification, logging, deletion, isolation, or cleaning.
- Supports Windows NT services and the NTFS (NT file system).
- Offers flexible scheduling and immediate (on-demand) scanning options.

Administrative ease

- Remote management of other NT workstations and servers through the AntiVirus Console lets administrators remotely change configurations of products, add/remove tasks, and initiate on-demand scans.

- NetShield's advanced alerting features include alphanumeric pager, e-mail via SMTP, SNMP, DMI, sound, network broadcast, program execution, and NT event logging.
- NetShield lets you send centralized alerts and reports from both workstations and servers.
- The Scan Wizard assists users in creating new scan tasks.
- The AutoUpdate feature allows immediate or scheduled updating via a central shared location or FTP download.
- The Service Password command-line utility lets administrators set or change the user ID and passwords used by McAfee Services on one or more systems.
- The Web-based Virus Information Library provides comprehensive virus information to users.

How To Contact Network Associates

Customer service

To order products or obtain product information, we invite you to contact our Customer Care department by calling (408) 988-3832 or by writing to the following address:

Network Associates, Inc.
2805 Bowers Avenue
Santa Clara, CA 95051-0963
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://www.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
Network Associates BBS	(408) 988-4004 1200 bps to 28,800 bps 8 bits, no parity, 1 stop bit 24 hours, 365 days a year
CompuServe	GO MCAFEE

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.

International contact information

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

Network Associates Canada

139 Main Street, Suite 201

Unionville, Ontario

Canada L3R 2G6

Phone: (905) 479-4189

Fax: (905) 479-4540

Network Associates Europe B.V.

Gatwickstraat 25

1043 GL Amsterdam

The Netherlands

Phone: 31 20 586 6100

Fax: 31 20 586 6101

Network Associates France S.A.

50 rue de Londres

75008 Paris

France

Phone: 33 1 44 908 737

Fax: 33 1 45 227 554

Network Associates Deutchland GmbH

Industriestrasse 1

D-82110 Germering

Germany

Phone: 49 8989 43 5600

Fax: 49 8989 43 5699

Network Associates (UK) Ltd.

Hayley House, London Road

Bracknell, Berkshire

RG12 2TH

United Kingdom

Phone: 44 1344 304 730

Fax: 44 1344 306 902

Network Associates Japan Co, Ltd.

Toranomon 33 Mori Bldg.

3-8-21 Toranomon

Minato-Ku, Tokyo 105

Japan

Phone: 81 3 5408 0700

Fax: 81 3 5408 0780

Network Associates Korea

135-090, 18th Fl.,
Kyoung Am Bldg.

157-27 Samsung-Dong,
KangamKu

Seoul, Korea

Phone: 82 2 555-6818

Fax: 82 2 555-5779

Network Associates South East Asia

7 Temasek Boulevard

The Penthouse

#44-01, Suntec Tower One

Singapore 038987

Phone: 65 430-6670

Fax: 65 430-6671

Network Associates Latin America

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

United States

Phone: (954) 452-1731

Fax: (954) 236-8031

Network Associates Australia

Level 1, 500 Pacific Highway

St. Leonards, NSW 2065

Australia

Phone: 61-2-9437-5866

Fax : 61-2-9439-5166

BBS: 61-2-9439-5640

Internet: http://www.nai.com.au

Reporting new viruses for NetShield updates

Network Associates is committed to providing you with effective and up-to-date tools you can use to protect your system. To that end, we invite you to report any new viruses that your software does not now detect. Please note that Network Associates reserves the right to use any information you supply as it deems appropriate, without incurring any obligations whatsoever. Send your suggestions and virus samples to:

virus_research@cc.mcafee.com

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

virus_research_europe@cc.mcafee.com

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

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

avert-jp@ccj.mcafee.com

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

avert_apac@ccj.mcafee.com

2 Installing NetShield

Overview

The NetShield installation procedure has two parts:

- installing the NetShield program
- setting up NetShield tasks

Although you can scan and clean files, folders, diskettes, or drives using the NetShield application, you do not have to launch the Netshield program in order for NetShield to perform automated tasks. You can create automated tasks using the Scan Config Wizard or directly through the AntiVirus Console. See Chapter 4, “Using the AntiVirus Console.”

Before You Start

Before you install NetShield, be sure you are logged onto the Windows NT network with administrator access. Then review the basic requirements for installing NetShield.

System requirements

✍ *NetShield is a Windows NT service; no additional memory is required to run the software. However, the amount of system resources used varies. By specifying scanning priority for each task, you determine the amount of system resources the program uses.*

Local installation

To install NetShield on a local server, you must have:

- a Windows NT server version 3.51 or later

  OR

  a Windows 95 system (the AntiVirus Console is the only installable component for Windows 95 systems)

- the latest version of Microsoft Service Pack for Windows NT is recommended

- at least 6MB of free disk space to install the program files.

Remote or silent installation

To install NetShield on remote servers or workstations in your network, you must have:

- a Windows NT server and workstation version 3.51 or later
- the latest version of Microsoft Service Pack for Windows NT is recommended
- 6MB or less, depending upon the NetShield components you want to install

Performing a Local Installation

NetShield is BackOffice compliant and supports multiple installations through the use of SMS. For information on using SMS, refer to the documentation that accompanied Windows NT.

Follow these steps to install NetShield on a local server:

Step	Action

1. Log on to the Windows NT server. You must have Administrator privileges to the Windows NT server.

2. To install from compact disc, insert it into your CD-ROM drive.

OR

To install from files downloaded from a BBS or the Network Associates website, decompress the zipped files into a directory on the network or your local drive.

3. Double-click the SETUP.EXE program in File Manager, or run one of the following commands from the Windows NT command line:

- If installing from the CD, enter the following command:

  `x:\SETUP`

  where *x* is the drive that contains the CD.

- If installing from files you downloaded from the Network Associates website, enter the following command:

  `x:\path\SETUP`

  where *x:path* is the drive and directory where you decompressed the files.

Response: The NetShield for Windows NT License Agreement screen is displayed. Read it carefully before proceeding with the installation.

4. Click Yes to begin the installation.

Response: The NetShield for Windows NT welcome screen is displayed.

5. Click Next.

   Response: The Installation Destination screen appears.

6. Select Local Installation to install NetShield on this server. If you want to perform a remote installation to other computers on your network, see "Performing a Remote Installation" on page 26 for instructions.

7. Click Next.

   Response: The Setup Type screen appears.

8. Select the destination directory for the NetShield program files.

9. Select the type of installation:

   - To install NetShield with the most common options, select Typical, then click Next.
   - To configure NetShield to use the fewest resources, select Compact, then click Next.
   - To perform a custom installation, select Custom, then click Next. Select components to install and system options, then click Next.

10. At the Service Account Information screen, select one of these options:

    - **Use the System Account.** Select this option if you do not want to use a custom account during installation. If this option is selected, NetShield will only be able to access the resources available on this computer.
    - **Use the Custom Account.** Select this option to enable NetShield to access network resources such as alert forwarding and automatic updates. Enter a user name (e.g. *domain**user name*) and a password with administrator rights in the text box provided.

11. Click Next to continue.

12. Verify that the installation options are correct, then click Next.

    Response: NetShield copies its program files to the remote computers where it uninstalls any existing NetShield files and installs the new files.

Performing a Remote Installation

NetShield is BackOffice compliant and supports multiple installations through the use of SMS. For information on using SMS, refer to the documentation that accompanied Windows NT.

Follow these steps to install NetShield or components of NetShield on remote computers in your network:

Step **Action**

1. Log on to a Windows NT server. You must have Administrator privileges to this server.

2. To install from compact disc, insert it into your CD-ROM drive.

   OR

   To install from files downloaded from a BBS or the Network Associates website, decompress the zipped files into a directory on the network or your local drive.

   ✍ *A remote installation cannot be performed from files copied to floppy diskettes. If you do not have the NetShield CD-ROM, install from files on your network or local drive.*

3. Double-click the SETUP.EXE program in File Manager, or run one of the following commands from the Windows NT command line:

   - If installing from the CD, enter the following command:

     `x:\SETUP`

     where *x* is the drive that contains the CD.

   - If installing from files you downloaded from the Network Associates website, enter the following command:

     `x:\path\SETUP`

     where *x:path* is the drive and directory where you decompressed the files.

   Response: The NetShield for Windows NT License Agreement screen is displayed. Read it carefully before proceeding with the installation.

4. Click Yes to begin the installation.

   Response: The NetShield for Windows NT welcome screen is displayed.

5. Click Next to open the Installation Destination screen. Select Remote Installation to install NetShield, or components of NetShield, to computers on your network.

6. Click Next, then enter the name of the remote Windows NT computer that you want to install NetShield to in the New Computer text box. Click the Browse button to navigate to the computer, then click ADD.

   Response: The Remote Installation Information screen appears (Figure 2-1).

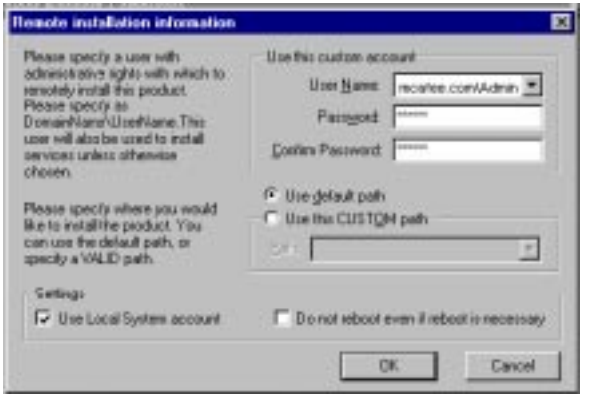


Figure 2-1. Remote Installation Information screen

7. Enter a domain name and user name with administrator rights in the User Name text box. Enter a password in the Password and Confirm Password text boxes. Repeat step 6 and step 7 to add computers to the installation.

8. Select Use Default Path to install NetShield files to the default directory (x:\Windows\Program Files\McAfee\NetShield).

   Select Use Custom Path to install NetShield files to a different location. Enter the complete path to where you want the NetShield files installed.

9. Select Use Local System Account to use the Service Account settings configured on the local system.

10. Select Do Not Reboot Even If Reboot Is Necessary if you do not want the remote computer restarted after installation.

    Response: The Confirm Installation Settings screen appears.

11. Verify that the installation options are correct, then click Next.

    Response: NetShield copies its program files to the remote computers, where it uninstalls any existing NetShield files and installs the new files.

12. When NetShield completes the installation on all computers, a confirmation screen appears listing successful or unsuccessful installations. Click Finish.

Performing a silent installation

To perform a "silent" installation of this product, with minimal user interaction and with all default or "Typical" installation settings, follow the instructions for performing a remote installation and add `-s` to the setup command (`i.e., SETUP.EXE -s`)when you install the product.

Customizing the silent installation

Follow these steps to customize the silent installation feature:

Step	Action
1.	Check the Windows directory to ensure that a file named SETUP.ISS does not already exist. If one does, rename it, back it up, or delete it.
2.	From the Start menu, select Run and enter the following command to record your installation settings: `SETUP.EXE -r`
3.	Select the components you want to install during the silent installation.
4.	Finish the installation, and locate the SETUP.ISS file in the Windows directory.

Your installation settings are recorded in the SETUP.ISS file. Use this file to install all NetShield files to the same installation directory on every client machine. The SETUP.ISS file contains the following information:

```
[InstallShield Silent]
  Version=v3.00.000
  File=Response File
[DlgOrder]
  Dlg0=SdLicense-0
  Count=6
  Dlg1=SdWelcome-0
  Dlg2=SdSetupType-0
  Dlg3=_USR_SdAskNameAndPassword2-0
  Dlg4=SdStartCopy-0
  Dlg5=SdFinishReboot-0
[SdLicense-0]
  Result=1
[SdWelcome-0]
  Result=1
[SdSetupType-0]
  szDir=C:\Program Files\McAfee\NetShield
  Result=401
[_USR_SdAskNameAndPassword2-0]
  szUserName=
  szPassword=
  nIsBDC=0
  Result=5
[SdStartCopy-0]
  Result=1
[Application]
  Name=NetShield NT
  Version=3.1.4
```

```
Company=McAfee
[SdFinishReboot-0]
Result=1
BootOption=1
```

The .ISS file defines the NetShield installation directory under the [SdSetupType-x] section.

Example:

```
[SdSetupType-0]

szDir=C:\Program Files\McAfee\NetShield
```

The szDir setting overrides the default installation directory on each client machine (which may vary according to the operating system). Use the same directory name on every client machine to help ease administration in the future; for example, assign all client machines the directory C:\ANTIVIRUS.

If, however, you want the SETUP.EXE program to determine a location for the NetShield files, you must modify the SETUP.ISS file to tell the target machine to ignore the szDir setting. To do this, follow these steps:

1. Open the SETUP.ISS file located in the Windows directory.
2. Locate the [SdSetupType-x] section and go to the line:

   ```
   Result = xxx
   ```

   The actual value specified here might be 301, 302, or 303, depending on what options you selected during the ISS file creation process. Add 100 to this number, for example, 301 becomes 401. This tells each target machine to disregard the szDir and assign a directory according to its own particular operating system.
3. Save and exit the SETUP.ISS file.

4. Copy the NetShield installation files onto a local or mapped drive; then rename, back up, or delete the SETUP.ISS file.

   ✍ *You cannot perform a silent install from multiple media. The silent operation will be compromised when the install prompts the user for more media.*

5. Copy the new SETUP.ISS file from the Windows directory to the location of the NetShield installation files.

   ✍ *The file used for the silent installation, SETUP.ISS, is product-specific. For example, you cannot use a SETUP.ISS file created by a VirusScan for Windows 95 installation for a NetShield for Windows NT installation.*

6. From the Start menu, select Run and enter the following command:

   ```
   SETUP.EXE -s
   ```

   ✍ *If you do not specify a "recorded" answer for all dialog boxes during the initial installation, the silent installation will not be successful.*

7. When the silent installation is complete, the machine reboots automatically.

3 Getting Started

Launching the AntiVirus Console

NetShield for Windows NT is a client-server application consisting of the AntiVirus Console on the client side and the NetShield Server software on the server side. The Console configures and controls the Server software and may run on the server or any attached workstation for remote anti-virus management. In addition to configuring and controlling functions, the Console can also receive information such as statistics and alarm notifications.

After installation, all NetShield configuration and management is controlled through the AntiVirus Console. This chapter outlines the options that are available using the AntiVirus Console.

To start the AntiVirus Console, do one of the following:

- In Windows NT 3.51, open the NetShield group in the Program Manager, and double-click the AntiVirus Console icon.
- In Windows NT 4.0, click Start in the taskbar, point to NetShield in the Programs menu, and click AntiVirus Console.

Response: The AntiVirus Console appears with these components:

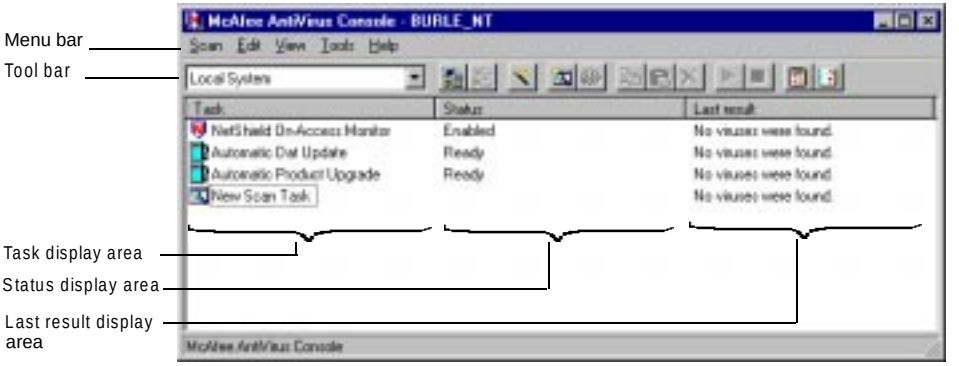


Figure 3-1. AntiVirus Console

The task display area

The task display area is the main part of the Console containing all defined tasks. The on-access task is always shown at the top of the display area.

Other tasks appear as you create them. To create a new on-demand task, see "Creating an on-demand task" on page 53.

To edit the on-access task, see "Editing the on-access task" on page 41.

✍ *To display a task's statistics, double-click the task. This is equivalent to highlighting a task and selecting Statistics from the Scan menu.*

The status bar

As you move the cursor around the Console, the status bar contains information about the current item.

The last results display area

The last results display area lists the latest task results.

Remote Administration

When the AntiVirus Console is started, the name of the server it is connected to is displayed on the Console title bar (unless you are running the Console on the server being configured). To administer a remote computer running NetShield, complete the following steps:

Step	Action

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

Response: The Connect to Remote Computer dialog box appears (Figure 3-1).

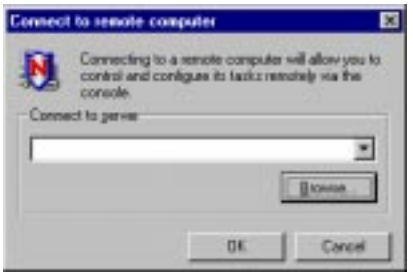


Figure 3-1. Connect to Remote Computer dialog box

2. Enter the name of the server that you want to connect to in the text box. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the computer on the network. The target server must have the NetShield server software for Windows NT or Novell NetWare installed.

✍ *The NetShield options available may vary according to the platform.*

3. Click OK.

Response: The name of the new server appears in the Console title bar and any configured tasks appear in the Console task window (tasks for other servers disappear).

4 Using the AntiVirus Console

Most of the functionality of NetShield is built into the AntiVirus Console. From the Console, you can configure and schedule tasks that monitor the server workstation or scan local or network drives.

What Is a Task?

A task is a powerful utility that can scan for viruses and update old NetShield files according to how it is configured. NetShield performs three types of tasks: on-access tasks, on-demand tasks, and AutoUpdate tasks.

The on-access task monitors files accessed or copied from the server (via network connections and floppy diskettes). The administrator may specify what types of files are scanned and how NetShield responds to infected files. For information on editing the on-access task, see “Editing the on-access task” on page 41.

On-demand tasks are drive-scanning tasks. On-demand tasks can be scheduled to automatically scan network drives or even individual workstation drives. The administrator may specify what files are scanned, how often a scan takes place, and how NetShield responds to infected files. For information on creating an on-demand task, see “Creating an on-demand task” on page 53.

The AutoUpdate tasks automatically download updates and upgrades from an ftp site or network distribution site. After the NetShield files are downloaded, AutoUpdate can either post them to a distribution site for downloading by other computers or automatically apply the new files to your NetShield machines. For information on creating the AutoUpdate tasks, see Chapter 8, “Updating NetShield.”

Working with Tasks

NetShield is designed to be easy-to-use and flexible. This section describes many of the features that enable you to view task statistics, import and export tasks, and copy and paste tasks.

Using the Statistics window

The Statistics window displays a task's current status and statistics on files scanned. To open the Statistics window, double-click a task, or highlight a task and select Statistics from the Scan menu.

Importing and exporting tasks

NetShield supports the importing and exporting of task configurations through the .VSC (Virus Scanning Configuration) file. This enables you to save tasks, move tasks to another computer, or import tasks from another computer.

✍ *For information on the .VSC file format, see "VSC File Format" on page 177.*

NetShield includes the IMPTASK utility for exporting .VSC files to multiple servers. For more information, see "Using the IMPTASK utility" on page 158.

Exporting

Follow these steps to export a task:

Step	Action
1.	Highlight an on-demand task.
2.	Select Export from the Edit menu.
	Response: The Select Export File dialog box appears.

3. Enter a path and filename. Click OK.

   Response: You receive a message confirming successful export. Click OK.

Importing

Follow these steps to import a task:

Step	Action

1. Select Import from the Edit menu.

   Response: The Import File dialog box appears.

2. Browse for a .VSC file to import.

3. Click Open.

   Response: The file appears as “New Scan Task” in the Console window.

4. Enter a name for the new file. Click OK.

   Response: The Task Properties dialog box appears.

5. Make any necessary changes to the task, then click OK.

Copying and pasting tasks

To quickly configure multiple computers and save time, NetShield supports the copying and pasting of tasks. Follow these steps to copy a task:

Step	Action
1.	Highlight the task to copy, then click  or select Copy from the Edit menu.
2.	To copy the task to this computer, continue to the next step. OR To copy the task to another computer, connect to the computer. For information on connecting to another computer, see “Remote Administration” on page 34.
3.	Click  or select Paste from the Edit menu. **Response**: The task appears as “New Scan Task” in the Console window.
4.	Enter a name for the task, then press ENTER. **Response**: The Task Properties dialog box appears.
5.	Make any necessary changes to the task, then click OK.

✍ *Only on-demand tasks may be copied. The on-access task cannot be copied.*

Disabling tasks

Disabling the on-access task

To disable the on-access task, highlight the task, and select Disable from the Scan menu.

Disabling on-demand tasks

To disable an on-demand task without deleting, simply disable the scheduler. For information about using the scheduler, see “Creating an on-demand task” on page 53.

Deleting tasks

Deleting the on-access task

The on-access task cannot be deleted. To disable the on-access task, see “Disabling tasks,” above. To change the properties of the on-access task, see “Editing the on-access task” on page 41.

Deleting on-demand tasks

To delete an on-demand task, highlight a task, and select Delete from the Scan menu.

5 On-access Scanning

The On-access Task

NetShield's on-access scanning provides real-time protection for your system. On-access scanning helps to prevent virus infection by automatically checking items—such as files, directories, drives, and any media—as they are accessed. Use the on-access task to configure these settings. See the following sections for detailed instructions on creating and editing the on-access task.

Viewing on-access status

When NetShield is enabled, you can configure your scanning options or view the status of files scanned from the NetShield Statistics window (Figure 5-1). To display this window, double-click the NetShield icon on the taskbar.

Figure 5-1. NetShield Statistics

Editing the on-access task

The on-access task appears in the AntiVirus Console task window and is preceded by a shield ( ). Although the on-access task may be disabled, it cannot be deleted.

Figure 5-2. AntiVirus Console

To edit the on-access task, highlight the task and click  or right-click the task and select Properties from the popup menu.

Response: The NetShield Properties dialog box appears with the Detection property page displayed

.

Figure 5-3. NetShield Properties dialog box (Detection page)

Configuring scan options

To define the scope of the on-access scan, you can specify which files NetShield should scan for viruses, enable or disable scanning at startup, and determine if users are allowed to disable NetShield. Use the Detection page to define the scope of the scan.

To tell NetShield what to scan, follow these steps:

Step	Action
1.	Highlight the on-access task in the AntiVirus Console and click  .

Response: The NetShield Properties dialog box appears with the Detection page displayed (Figure 5-3).

2. Select which files to scan:

   - **Inbound Files.** Select the Inbound Files checkbox to scan all files written or modified on the server.
   - **Outbound Files.** Select the Outbound Files checkbox to scan files read from the server.
   - **Floppy during Shutdown.** This tells NetShield to scan the floppy drive on your computer before the system is shutdown. Enable this option to prevent the spread of viruses by users rebooting with an infected floppy in the drive.
   - **Compressed Files.** This tells NetShield to can files compressed with PKLITE and LZEXE.

3. Specify whether you want NetShield to examine all files, only those files most susceptible to virus infection, compressed files, or network drives by choosing these options from the What to Scan list:

   - **All Files**. This tells NetShield to scan every file type. This option is your best protection against infection.
   - **Program Files Only**. This tells NetShield to scan only the files that are most susceptible to virus infection. Click the File Types button to specify the filename extensions that NetShield uses to identify these files.

     Response: The Program File Extensions dialog box appears (Figure 5-4).

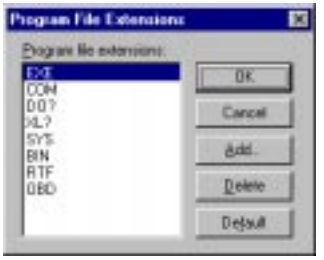


Figure 5-4. Program File Extensions dialog box

✍ *By default, NetShield identifies files with the extensions .EXE, .COM, .DO?, .XL?, SYS., BIN., RTF, and ODB. as most susceptible to virus infection. It uses the extensions .DO?, and .XL? to identify Microsoft Word and Excel document and template files, which can contain macro viruses. The ? character is a wildcard.*

- To add a file extension, click Add. Enter a new file extension to scan and click OK. Repeat this procedure until all desired file extensions are entered.
- To delete an extension, highlight it and click Delete.
- To return to the default extensions, click Default.

When you are finished editing the list of file extensions, click OK.

- **Network Drives.** This tells NetShield to scan files as they are accessed on mapped or UNC network drives.

4. Select the Enable On-Access Scanning at System Startup checkbox to tell NetShield to automatically start scanning each time the computer is started.

✍ *To manually start or stop the NetShield service, use the Services Manager located in the Control Panel. For more information, refer to the documentation that accompanied Microsoft NT.*

5. Select the Users Are Allowed To Disable NetShield checkbox to allow disabling of the on-access task from the AntiVirus Console.

6. Select the Enable File Scan Caching checkbox to improve over-all on-access scanning performance of NetShield. When this option is enabled, NetShield will only scan files the first time they are accessed after the system or Task Manager is restarted. If a file in the cache is modified, NetShield will rescan the file.

7. To further configure this task, select another dialog page. To save the changes and return to the AntiVirus Console, click OK. To cancel any changes and return to the AntiVirus Console, click Cancel.

Responding to infections

NetShield can prevent the spread of an infection by automatically cleaning, deleting, relocating or denying access to infected files. Use the Actions property page (Figure 5-5) to tell NetShield what to do when it finds a virus.

To configure NetShield's response to a virus infection, follow these steps:

Step	Action
1.	Highlight the on-access task in the AntiVirus Console and click  .
2.	Click the Actions tab.
	Response: The Actions page (Figure 5-5) appears..

Figure 5-5. NetShield Properties dialog box (Actions page)

3. Select NetShield's response to a detected virus from the When a Virus is Found pull-down list. Your choices are:

- **Deny access to the infected files and continue.** This option is recommended for systems left unattended. When this option is enabled, NetShield denies user access to the infected files existing on the server and appends infected files written to the server with a .VIR extension.

  ✍ *Confirm that report logging is enabled. This will ensure you have a record of which files were locked, so you can clean them or restore them from backups.*

- **Move infected files to a folder.** Use this option to tell NetShield to move infected files to a “quarantine” folder.

  - Enter the name of the quarantine folder that will receive forwarded messages in the Folder To Move To text box. You can enter the folder name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the folder on the network.

  ✍ *If an infected file cannot be cleaned or if NetShield does not have the proper file access, file access will be denied.*

- **Clean infected files automatically.** This option is enabled by default.

  ✍ *If a virus cannot be removed from a file or the file is damaged beyond repair, NetShield automatically denies access to the file. If this occurs, delete the file and restore the original from backups. See “Logging on-access scan activity” on page 48.*

- **Delete infected files automatically.** Use this option to tell NetShield to delete infected files as soon as it detects them.

  ✍ *If you select this option, confirm that activity logging is enabled. This will ensure you have a record of which files were deleted, so you can restore them from backups. See “Logging on-access scan activity” on page 48.*

4. To configure NetShield to send a disconnect message to the infected computer, select the Send Message to User checkbox and enter a custom message.

5. Select the Disconnect Remote Computers and Deny Access to Network Share checkbox to configure NetShield to disconnect infected remote computers.

6. To further configure this task, select another property page. To save the changes and return to the Console, click OK. To cancel any changes and return to the Console, click Cancel.

Logging on-access scan activity

The NetShield on-access activity log, *NETSHIELD ACTIVITY LOG.TXT,*keeps track of NetShield's on-access scan activity, including virus detection, virus cleaning, infected file deletion, infected file move, and session settings.

✍ *On-demand scan activity is logged in a separate logfile. See "Logging on-demand scans" on page 61 for information about the on-demand scan activity log.*

Use the Reports property page (Figure 5-6) to determine what information is included in the logfile.

To configure logfile settings, follow these steps:

Step	Action
1.	Highlight the on-access task in the AntiVirus Console and click  .
2.	Click the Reports tab. **Response**: The Reports page appears (Figure 5-6 on page 49).

Figure 5-6. NetShield Properties dialog box (Reports page)

3. Select the Log to File checkbox. Next, type the filename and path for your logfile in the text box provided, or click Browse to designate a location to store it.

✍ *The default on-access task logfile is NETSHIELD ACTIVITY LOG.TXT and is located in the McAfee\ NetShield directory.*

4. Select the Limit Size of logfile checkbox to keep the logfile from using excessive hard disk space. Specify a size between 10KB and 99999KB. By default, NetShield sets a limit of 100KB.

5. Select the information you want NetShield to record in the logfile. Your available log options will depend on the action set. See "Responding to infections" on page 45, to configure NetShield's actions. Your possible choices are:

   - Virus Detection
   - Virus Cleaning
   - Infected File Deletion
   - Infected File Move
   - Session Settings
   - Session Summary
   - Date and Time
   - User Name

6. To further configure this task, select another property page. To save the changes and return to the Console, click OK. To cancel any changes and return to the Console, click Cancel.

Excluding folders from being scanned

NetShield can exclude the files, folders, and drives that you choose from scanning. Use the Exclusion property page (Figure 5-7 on page 51) to define which files, folders, or drives will be excluded from on-access virus scanning.

✍ *If NetShield is configured to automatically move infected files to a quarantine folder, the folder is automatically excluded from scanning.*

To exclude files, folders, or drives from being scanned, follow these steps:

Step	Action
1.	Highlight the on-access task in the AntiVirus Console and click  .
2.	Click the Exclusions tab. **Response**: The Exclusions page appears (Figure 5-7 on page 51).

.

Figure 5-7. NetShield Properties dialog box (Exclusions page)

3. Click Add to add an item to the Exclusion list.

Response: The Exclude Item dialog box appears (Figure 5-8).

Figure 5-8. Exclude Item dialog box

4. Type the drive letter, the path to the file, or the path to the folder you wish to exclude from scanning, or click Browse to locate the folder.

5. Select the Include Subfolders checkbox, to exclude all subfolders within the selected folder.

6. Select the Inbound checkbox to exclude the item from inbound scanning (files modified on or written to the server).

   Select the Outbound checkbox to exclude the item from outbound scanning (files read from the server).

7. Repeat steps 1 through 6 until all items to be excluded are entered.

8. To edit an item, highlight the item in the Exclusions list and click Edit.

9. To delete an item, highlight the item in the Exclusions list and click Remove.

10. To further configure this task, select another property page. To save the changes and return to the Console, click OK. To cancel any changes and return to the Console, click Cancel.

6 On-demand Scanning

On-demand Tasks

With an on-demand scan task you can perform immediate and scheduled scans of specific items while you're working. NetShield's on-demand scanner allows you to scan new media or specific files to determine whether a computer virus is present. NetShield immediately detects boot, file, macro, stealth, encrypted, and polymorphic viruses located within files, drives, and diskettes.

Creating an on-demand task

To create a new on-demand task, click  or select New Task from the Scan menu.

Response: A new on-demand task appears in the AntiVirus Console task window.

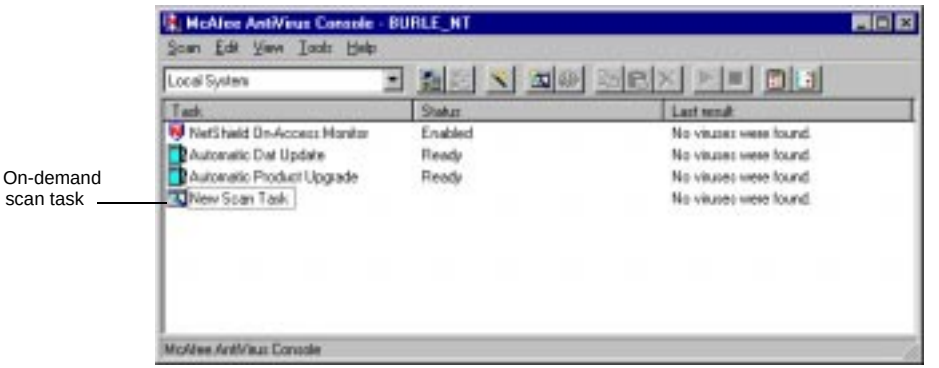


Figure 6-9. AntiVirus Console

Editing an on-demand task

To edit the name of the on-demand task, highlight the text with your mouse and type a new name over “New Scan Task.“

To edit the on-demand task scan settings, highlight the task and click  .

Response: The Task Properties dialog box appears with the Detection property page displayed (Figure 6-10).

Figure 6-10. Task Properties dialog box (Detection page)

Selecting file types and locations for scanning

Use the Detection property page (Figure 6-10) to configure which items should be scanned. Following these steps to configure your detection options:

Step	Action

1. Highlight the on-demand task in the AntiVirus Console and click  .

   Response: The Task Properties dialog box appears with the Detection page selected (Figure 6-10 on page 54).

2. Click the Add a Scan Item button.

   Response: The Add Scan Item dialog box appears (Figure 6-11).

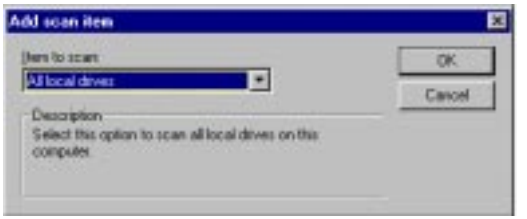


Figure 6-11. Add Scan Item dialog box

3. To add an item to the scan list, select it from the Item to Scan pull-down list. You can choose from:

   - **All Local Drives.** This option tells NetShield to scan all local hard drives.
   - **Drive or Folder.** This option tells NetShield to scan the selected drive or folder. Specify the path to the drive or folder you want to scan. Use the Browse button to navigate to the drive or folder you want NetShield to scan.
   - **File.** This option tells NetShield to scan the selected file. Specify the path to the file you want to scan. Use the Browse button to navigate to the file you want NetShield to scan.

4. Click OK.

   Response: The items you selected appear in the Selections list.

5. To remove an item from the list to be scanned, select it from the list and click Remove.

6. Select the types of files you want NetShield to check for viruses.

   - **Compressed Files.** This tells NetShield to scan files compressed with PKLITE, LZEXE, PKZIP, LHA, LZH and MS-CAB.
   - **All Files**. This tells NetShield to scan every file in the drive or folder that you specified.
   - **Program Files Only**. This tells NetShield to scan only the files that are most susceptible to virus infection. Click the Program Files button to specify the filename extensions that NetShield uses to identify these files.

     Response: The Program File Extensions dialog box appears (Figure 6-12).

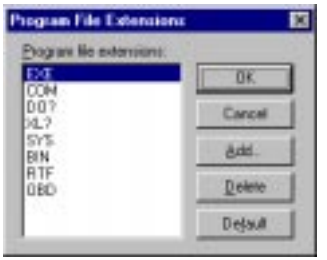


Figure 6-12. Program File Extensions dialog box

✍ *By default, NetShield identifies files with the extensions .EXE, .COM, .DO?, .XL?, .SYS, .BIN, .RTF, and .OBD as most susceptible to virus infection. It uses the extensions .DO?, and .XL? to identify Microsoft Word and Excel document and template files, which can contain macro viruses. The ? character is a wildcard.*

- To add a file extension, click Add. Enter a new file extension to scan and click OK. Repeat this procedure until all desired file extensions are entered.

- To delete an extension, highlight it and click Delete.
- To return to the default extensions, click Default.

When you are finished editing the list of file extensions, click OK.

- **Include Subfolders.** This tells NetShield to scan subfolders within the drive or folder you specified.

7. Click the Advanced button to set the scan priority level and to set scan exclusion options.

Response: The Advanced Scanner Settings dialog box appears.

Figure 6-13. Advanced Scanner Settings dialog box

- In the Priority Level section, drag the slider to the right to perform high priority scans. High priority scans are thorough scans and may take longer to complete. Drag the slider to the left to perform lower priority scan.

- Select the Skip Boot Record Scanning checkbox to skip the scanning of the systems boot record.

- Select the Skip Memory Scanning checkbox to skip the scanning of the systems memory.

8. To further configure this task, select another property page. To save the changes and return to the Console, click OK. To cancel any changes and return to the Console, click Cancel.

Setting NetShield's response to a virus infection

NetShield can prevent the spread of an infection by automatically cleaning, deleting, continue with the scan task, or relocating infected files. Use the Actions property page (Figure 6-14) to tell NetShield what to do when it finds a virus.

To configure NetShield's response to a virus infection, follow these steps:

Step	Action
1.	Highlight the on-demand task in the AntiVirus Console and click  .
	Response: The Task Properties dialog box appears.
2.	Click the Actions tab.

Response: The Actions property page appears (Figure 6-14)..

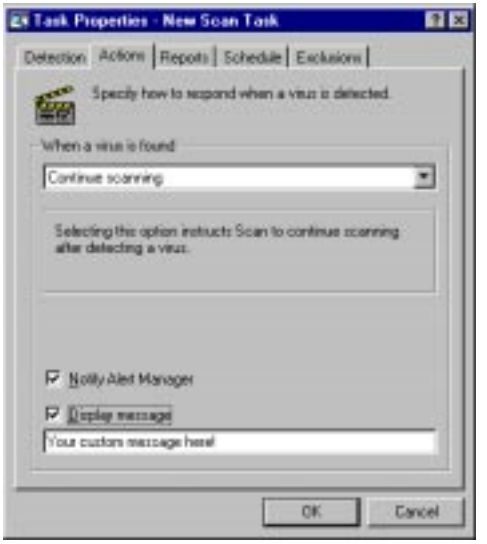


Figure 6-14. Task Properties dialog box (Actions property page)

3. Select NetShield's response to a detected virus from the When a Virus is Found pull-down list. Your choices are:

   - **Continue scanning.** Choose this option to tell NetShield to continue with the scan task after a virus is detected.

     ✍ *If this option is selected for a scheduled scan task, be sure to view the Last Results column in the Console to check the results of the scan or check the NetShield scan logs for infected files immediately after scanning.*

   - **Move infected files to a folder.** Use this option to tell NetShield to move infected files to a "quarantine" folder.

     - Enter the name of the quarantine folder that will receive forwarded messages in the Folder To Move To text box. You can enter the folder name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the folder on the network.

     ✍ *If an infected file cannot be cleaned or if NetShield does not have the proper file access, file access will be denied.*

   - **Clean infected files automatically.**

     ✍ *If a virus cannot be removed from a file or the file is damaged beyond repair, NetShield automatically denies access to the file. If this occurs, delete the file and restore the original from backups. See "Logging on-demand scans" on page 61.*

   - **Delete infected files automatically.** Use this option to tell NetShield to delete infected files as soon as it detects them.

     ✍ *If you select this option, confirm that activity logging is enabled. This will ensure you have a record of which files were deleted, so you can restore them from backups. See "Logging on-demand scans" on page 61.*

4. To configure NetShield to send a disconnect message to the infected computer, select the Send Message to User checkbox and enter a custom message.

5. Select the Disable User Account checkbox to configure NetShield to disconnect infected network connections.

   ✍ *Although disconnection takes place almost instantly, larger domains take longer to synchronize account information, and it is possible for a user to log back in. This is a function of the Windows NT operating system. For more information, refer to the documentation that accompanied Windows NT.*

6. To further configure this task, select another property page. To save the changes and return to the Console, click OK. To cancel any changes and return to the Console, click Cancel.

Logging on-demand scans

The NetShield on-demand scan activity log, SCAN ACTIVITY LOG.TXT, keeps track of NetShield's on-demand scanning activity, including virus detection, virus cleaning, infected file deletion, infected file move, and session settings.

✍ *On-access scan activity is logged in a separate logfile, NETSHIELD ACTIVITY LOG.TXT. See "Logging on-access scan activity" on page 48 for information about the on-access scan activity log.*

Use the Reports property page (Figure 6-15) to determine the information that will be included in the log entry.

To configure logfile settings, follow these steps:

Step	Action

1. Highlight the on-demand task in the AntiVirus Console and click  .

2. Click the Reports tab.

   Response: The Reports page appears (Figure 6-15 on page 62).

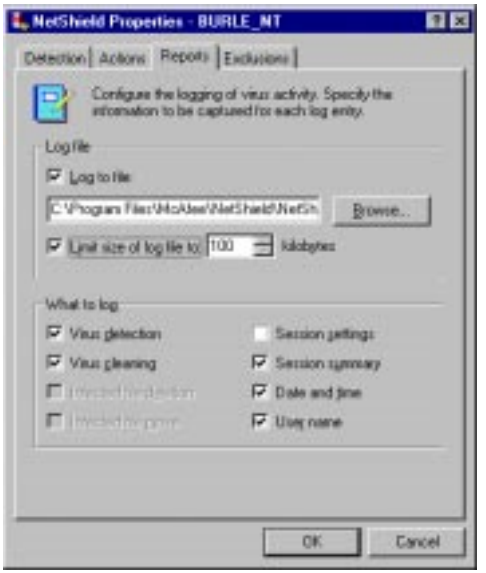


Figure 6-15. NetShield Properties dialog box (Reports page)

3. Select the Log to File checkbox. Next, type the filename and path for your logfile in the text box provided, or click Browse to designate a location to store it.

✍ *The default on-demand task logfile is SCAN ACTIVITY LOG.TXT and is located in the McAfee\ NetShield directory.*

4. Select the Limit Size of logfile checkbox to keep the logfile from using excessive hard disk space. Specify a size between 10KB and 99999KB. By default, NetShield sets a limit of 100KB.

5. Select the information you want NetShield to record in the logfile. Your available log options will depend on the action set. See "Setting NetShield's response to a virus infection" on page 58, to configure NetShield's actions. Your possible choices are:

   - Virus Detection
   - Virus Cleaning
   - Infected File Deletion
   - Infected File Move
   - Session Settings
   - Session Summary
   - Date and Time
   - User Name

6. To further configure this task, select another property page. To save the changes and return to the Console, click OK. To cancel any changes and return to the Console, click Cancel.

Scheduling the on-demand task

Scheduling allows you to configure an on-demand task to automatically start a scan at a predetermined time. This scan can happen once, daily, weekly, monthly, hourly, or each time the server is started.

Use the Schedule property page (Figure 6-16) to enable or disable the scheduler and to specify when the on-demand scan will run.

To schedule an on-demand scan, follow these steps:

Step	Action

1. Highlight the on-demand task in the AntiVirus Console and click  .

2. Click the Schedule tab.

   Response: The Schedule property page appears (Figure 6-16 on page 64).

Figure 6-16. Task Properties dialog box (Schedule page)

3. Select the Enable Schedular checkbox to enable the scheduled task. Once enabled, the default schedule is set to run monthly at 2:00A.M.

   ✍ *If this option is not enabled, the task will not run on schedule.*

4. Determine how often the task will run. Choose from these options:

   - **Once.** This tells NetShield to perform a one time scan at the time and date you specify. Enter the time and date the scan will run.

   - **Hourly.** This tells NetShield to perform a scan at the hour you specify. Set the scan task to start X minutes after the hour where X is a number between 0 and 59. For example, to set the scan to occur 30 minutes after every hour (8:30, 9:30, 10:30, etc.), click the Hourly button and type in 30.

   - **Daily.** This tells NetShield to perform a scan only on the days you specify. Enter the time for the scan to start, and click the Which Days button and select the days the scan will run. Click OK.

- **Weekly.** This tells NetShield to perform a scan once a week. Enter the time and day of the week the scan will run.
- **Monthly.** This tells NetShield to perform a scan once a month. Enter the time and day of the month the scan will run.
- **At Startup.** This tells NetShield to perform a scan every time the server is started.

5. Click OK.

6. To further configure this task, select another dialog page. To save the changes and return to the Console, click OK. To cancel any changes and return to the Console, click Cancel.

Excluding folders from being scanned

NetShield can exclude the files, folders, and drives that you choose from scanning. Use the Exclusion property page (Figure 6-17 on page 66) to define which files, folders, or drives will be excluded from on-access virus scanning.

To exclude files, folders, or drives from being scanned, follow these steps:

Step	Action

1. Highlight the on-access task in the AntiVirus Console and click  .

2. Click the Exclusions tab.

   Response: The Exclusions page appears (Figure 6-17 on page 66) with a list of all files, folders, and drives you have chosen to exclude from scanning.

   ✍ *The NetShield installation folder and PAGEFILE.SYS are automatically excluded from scanning and will appear in the Exclusion list. If NetShield is configured to move infected files to a quarantine folder, the folder is also excluded from scanning.*

.

Figure 6-17. Task Properties dialog box (Exclusions page)

To exclude files, folders, or drives from on-demand scans, follow these steps:

1. Click Add to add an item to the Exclusion list.

   Response: The Exclude Item dialog box appears (Figure 6-18).

Figure 6-18. Exclude Item dialog box

2. Type the drive letter, the path to the file, or the path to the folder you wish to exclude from scanning, or click Browse to locate the folder.

3. Select the Include Subfolders checkbox, to exclude all subfolders within the selected folder.

4. Select the Inbound checkbox to exclude the item from inbound scanning (files modified on or written to the server).

   Select the Outbound checkbox to exclude the item from outbound scanning (files read from the server).

5. Repeat steps 1 through 4 until all items to be excluded are entered.

6. To edit an item, highlight the item in the Exclusions list and click Edit.

7. To delete an item, highlight the item in the Exclusions list and click Remove.

8. To further configure this task, select another property page. To save the changes and return to the Console, click OK. To cancel any changes and return to the Console, click Cancel.

7 Virus Notification

In addition to automatically responding to viruses (cleaning, deleting, moving, etc.), NetShield may be configured to run a program on alert, maintain information in a local and/or remote event log(s), and alert personnel in a variety of ways (pagers, printers, e-mail, DMI, SNMP, etc.).

NetShield supports the use of any combination of notification methods and multiples of each. Alerts can also be forwarded from one computer to another.

- To configure NetShield to alert personnel of virus activity through pagers, printers, e-mail, Desktop Management Interface (DMI), forwarding, SNMP, etc., see “Using Alert Manager” on page 69.
- To configure NetShield to allow Centralized Alerting to report virus activity from workstations, see “Using Centralized Alerting” on page 99.
- To customize alert message text and priority levels, see “Customizing Alerts” on page 100.

Use the Alert properties sheet (Figure 7-1) to enable alerting and to configure Centralized Alerting settings. Select Alerts from the Tools menu to open the Alert properties sheet.

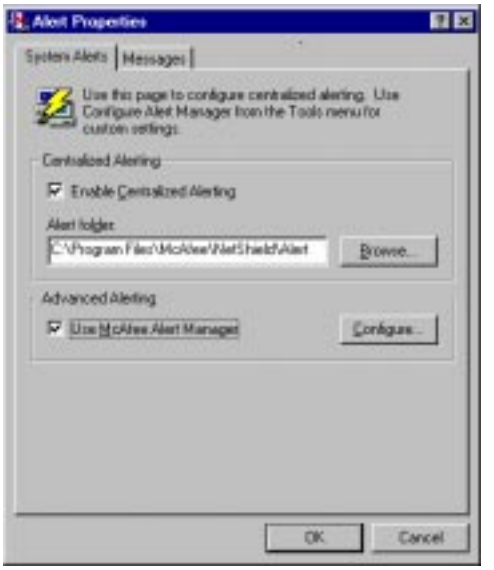


Figure 7-1. Alert Properties dialog box (System Alerts property page)

Using Alert Manager

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

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

✍ *In large organizations, use Forward to send alerts to centralized notification systems or to MIS departments to keep track of virus statistics and problem areas.*

To open the Alert Manager dialog box and choose configuration options, follow these steps:

Step	Action
1.	Start the AntiVirus Console, then select the Alerts option from the Tools menu. To learn how to start the AntiVirus Console, see “Launching the AntiVirus Console” on page 32. **Response**: The Alerts Properties page (see Figure 7-1 on page 69) appears.
2.	Select the Enable Alert Manager checkbox at the bottom of the page, then click OK.
3.	Select the Configure Alert Manager option from the Tools menu. **Response**: NetShield opens the Alert Manager dialog box Figure 7-2 on page 71 with the Summary tab selected. The Alert Manager dialog box includes nine different alert methods, each with configuration options shown in individual property pages. Click the tab corresponding to the alert method you want to configure to see the options available. When you have finished choosing your options, click OK to save your changes, close the Alert Manager dialog box, and return to the AntiVirus Console. Click Cancel to close the Alert Manager dialog box without saving your changes. The following sections describe the options available for each method.

Viewing the Summary page

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

The Summary page lists all of the alert methods you've told NetShield to use to notify you when it finds a virus or other malicious code on your NetShield server. In the example shown in Figure 7-2, the Alert Manager will generate DMI alerts, send a network message to computers specified, send alerts to a printer and pager. If you have not yet configured Alert Manager, the Summary Page will be blank.

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

See the following sections to learn more about the options available for each alert method.

Forwarding alerts to another computer

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

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

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

Response: The Forward page (Figure 7-3) appears with a list of all of the computers you have chosen 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), then enter the name of the computer that will receive forwarded messages in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the computer on the network. To choose additional options, continue with Step 4.

   - **Change configuration options.** Select one of the destination computers listed, then click Properties. Alert Manager opens the Forward Properties dialog box (Figure 7-4). 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.

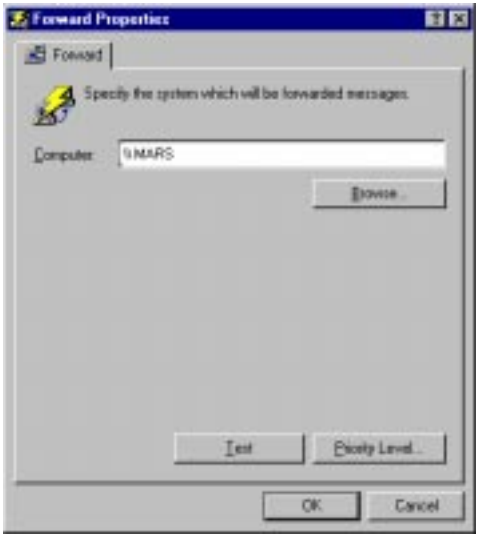


Figure 7-4. Forward Properties dialog box

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.

Figure 7-5. Priority Level dialog box

5. Click Test to send the destination computer a test message. The message will appear instantly on the destination computer's screen and the recipient will need to click OK to acknowledge it. If your recipient does not receive the message, check the Windows NT Event Viewer for an error message.

6. Click OK to return to the Alert Manager dialog box.

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

Sending a network message

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

To send alerts via network messages, your NetShield server must have the Alerter and Messenger Windows NT services running. The destination computers running Windows NT must have the Messenger service running to receive alert messages. Those running Windows 95 or Windows 3.1x must also be running the WinPopup utility to receive network messages. WinPopup comes with some Windows versions. See your Windows documentation for details.

Use the Network Message property page to send alert notifications via network messages and follow these steps:

Step	Action
1.	Open the Alert Manager Properties dialog box.
2.	Click the Network Message tab. **Response**: The Network Message tab appears (Figure 7-6)The Recipient list displays a list of all of the computers you have chosen to receive network messages. If you have not yet chosen any destination computers, 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/user**. Select one of the destination computers listed, then click Remove.
- **Add a computer/user to the list.** Click Add to open the Network Message Properties dialog box (Figure 7-7), then enter the name of 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.

  ✍ *If the specified name is both a valid username and computer, the alert message will be sent to the username.*

- **Change configuration options.** Select one of the destination computers 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 to learn how to choose new or different configuration options.

Figure 7-7. Network Message 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 74), 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 Network Message Properties dialog box.

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

   The message will appear instantly on the destination computer's screen and the recipient will need to click OK to acknowledge it. If your recipient does not receive the message, check the 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 configuration options and close the Alert Manager dialog box, click OK. To close the Alert Manager dialog box without saving changes, click Cancel.

Sending a SMTP alert to an e-mail address

Alert Manager can send the alert messages that NetShield generates to a recipient's e-mail address using standard Internet mail. The alert message appears 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.

Use the E-Mail property page to send alert notifications via e-mail and follow these steps:

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

Response: The E-Mail page (Figure 7-8 on page 78) appears with a list of the e-mail addresses to which you want to send alert messages. If you have not yet chosen any e-mail addresses, 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 (see Figure 7-9 on page 79). Enter the e-mail address for your alert recipient in the Address text box, enter a subject in the Subject text box, then enter your e-mail address in the From text box. Use the standard Internet address format *<username>@<domain>* (administrator_1@mail.com, for example). To choose additional options, continue with Step 4.

   - **Change configuration options.** Select one of the e-mail addresses listed, then click Properties. Alert Manager opens the E-Mail Properties dialog box (Figure 7-9 on page 79). 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: The message recipient receives a test message.

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 74), drag the slider to the right to send the recipient fewer, but higher priority, messages. Drag the slider to the left to send the recipient more messages, including lower priority messages. Next, click OK to save your changes and return to the E-Mail Properties dialog box.

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

Figure 7-10. SMTP dialog box

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

6. Click Test to send a test message to the e-mail address you entered. The message will appear in your recipient's mailbox.

7. Click OK to return to the Alert Manager Properties dialog box.

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

Sending an alert to a pager

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

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

Step	Action

1. Open the Alert Manager Properties dialog box.

2. Click the Pager tab.

   Response: The Pager page (Figure 7-11) appears with a list of the pager numbers to which you want to send alert messages. If you have not yet chosen any pager numbers, 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 83). Choose the type of pager your recipient uses from the list at the top of the page, then enter the information for that pager type in the text boxes provided.
  - If your recipient uses an alphanumeric pager, enter the pager number and, if necessary, the recipient's ID and password in the text boxes provided. Next, select the Use Alert Message button to send NetShield's standard alert message, or select the Use Custom Message button, then enter your custom message in the text box below.

- If your recipient uses a numeric pager, enter the pager number and the numeric message you want to send in the text boxes provided. Next, enter in the Delay box the number of seconds Alert Manager should wait before transmitting its message.
- 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 (see Figure 7-12 on page 83). 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 74), drag the slider to the right to send the recipient fewer, but higher priority, messages. Drag the slider to the left to send the recipient more messages, including lower priority messages. Next, click OK to save your changes and return to the Pager Properties dialog box.

5. Click Modem Settings to configure your modem to send pager messages. In the dialog box that appears (see Figure 7-13 on page 84), choose the type of modem connected to your server from the Modem list, the COM port it uses from the Port list, and the rate at which it can transmit data from the Baud list. Next, enter in the text boxes provided any dialing prefixes or suffixes the modem must dial to reach outside lines, use particular long-distance carriers, enter personal identification numbers or perform similar tasks.

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

Figure 7-13. Modem dialog box

6. Click Test to send a test message to the pager number you entered. If your recipient uses an alphanumeric pager, he or she will receive a text message from Alert Manager. If your recipient uses a numeric pager, he or she will see the telephone number or other message you specified in the Pager Properties dialog box.

7. Click OK to return to the Alert Manager Properties dialog box.

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

Sending an alert to a printer

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

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

Step	Action

1. Open the Alert Manager Properties dialog box.

2. Click the Printer tab.

   Response: The Printer page (Figure 7-14) appears with a list of all of the network printers you have chosen to receive alert messages. If you have not yet chosen any printers, this list will be blank. The printer must be configured by the Print Manager prior to configuring this notification option.

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 (Figure 7-15), then enter the name of the target printer in the text box provided. You can enter the printer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the printer on the network. To choose additional options, continue with Step 4.
- **Change configuration options.** Select one of the target printers 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 Computer 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 74), drag the slider to the right to send the destination printer fewer, but higher priority, messages. Drag the slider to the left to send the destination printer more network messages, including lower priority messages. Next, click OK to save your changes and return to the Printer Properties dialog box.

5. Click Test to send the destination printer a test message. The message will print as a simple, unformatted line of text.

6. Click OK to return to the Alert Manager Properties dialog box.

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

Using SNMP services

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

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

Step	Action
1.	Open the Alert Manager Properties dialog box.
2.	Click the SNMP tab. **Response**: The SNMP page (Figure 7-16) appears.
3.	Click the Enable SNMP Traps checkbox.

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

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 74), drag the slider to the right to send the SNMP management computer fewer, but higher priority, messages. Drag the slider to the left to send the SNMP management computer more messages, including lower priority messages. Next, click OK to save your changes and return to the Printer Properties dialog box.

To use this option, you must also install and activate the Windows NT SNMP service on the same machine that runs NetShield. If you have not yet done so, follow these steps:

Step	Action

1. Click Configure SNMP.

   Response: The Windows NT Network control panel dialog box appears. Click the Services tab to open the Services property page (Figure 7-17).

Figure 7-17. The Network control panel dialog box (Service page)

2. Click Add to install the Windows NT SNMP service, then follow the Microsoft installation instructions to complete your setup. You can find complete details in the Microsoft TCP/IP Help file included with Windows NT.

3. When you have finished installing the service, return to the Alert Manager's SNMP page.

4. Click Test to send the SNMP management computer a test message. To see the message you sent, start your SNMP viewer software.

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

Using DMI alerting

Alert Manager and DMI work together to alert the DMI management console instantly of a virus infection. When a virus is detected, DMI immediately generates an alert message for Alert Manager to display on the DMI management console.

✍ *DMI (Desktop Management Interface) is an industry interface for keeping track of and monitoring the status of components, including hardware and software, in the computers on your network. For more information about DMI, refer to your Intel documentation or visit the Desktop Management Task Force website at http://www.dmtf.org.*

To generate DMI alerts, your NetShield server must have the DMI software running.

Use the DMI property page to generate DMI alert notifications and follow these steps:

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

Response: The DMI page appears (Figure 7-18 on page 91).

Figure 7-18. Alert Manager Properties dialog box (DMI page)

3. Click the Enable DMI Usage checkbox. To use DMI alerting, this option must be enabled on the NetShield servers.

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 74), 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 DMI dialog box.

5. Click Test to generate a test message.

   Response: The test message immediately appears in the Event Monitor located in the DMI Component Test System.

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

Executing a program on alert

Alert Manager can be configured to launch any program or batch file on alert. For example, if your company is using cc:Mail or a special mail package that is not recognized by NetShield, you could write a batch file to send notifications to your mail package.

✍ *Any program launched from Alert Manager runs in the background without a visible user interface.*

To configure NetShield to execute a program on alert, follow these steps:

Step	Action
1.	Open the Alert Manager Properties dialog box.
2.	Click the Execute Program checkbox.

Response: The Program page (Figure 7-19) appears.

Figure 7-19. Alert Manager Properties dialog box (Program page)

3. Enter the name and path of the program you want NetShield to run upon detecting a virus. You can enter the program name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the program on the network.

   Alert Manager includes a virus notification utility, VIRNOTFY.EXE, that is launched by default when a virus is detected. The VIRNOTFY.EXE utility displays the Virus Notification dialog box which lists the location of the infected file and the virus name.

   ✍ *When Alert Manager launches a program, such as VIRNOTFY.EXE, these environment variables are initiated:*

   %INFFILENAME% - location of the infected file

   %VIRUSNAME% - name of the virus

   These environment variables can be used by the launched application for retrieving information about the infected file and the virus.

4. To execute the program on the first alert event only, click the First Time option button. To execute the program every time an alert event occurs, click the Every Time option button.

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

6. In the Priority Level dialog box (see Figure 7-5 on page 74), 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 Progam properties dialog box.

7. To test the launch of the program, click Test.

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

Using audible alerting

Alert Manager can use .WAV files to sound an audible alert on your system when NetShield detects a virus or when other alerts are generated.

✍ *To use this option, your system must have a sound card installed.*

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

Step	Action
1.	Open the Alert Manager Properties dialog box.
2.	Click the Sound tab. **Response**: The Sound page appears (Figure 7-20).

Figure 7-20. Alert Manager Properties dialog box (Sound page)

3. Click the Enable Audible Alerts checkbox.

4. In the text box provided, enter the name of the sound file you want Alert Manager to run when NetShield detects a virus. The sound file must have a .WAV extension. You can enter the file name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the file on your computer.

   Leave the text box blank to use the default system sound when NetShield detects a virus.

5. 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 74), 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 Sound Properties dialog box.

6. Click Test to send an audible alert test.

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

Logging with Alert Manager

Alert Manager can log the alert messages that NetShield generates to the computers it is running on or to other computers in your network to the Windows NT Event Log.

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

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

Response: The Logging page appears (Figure 7-21).The Recipient list displays a list of all of the computers you have chosen to receive alert logging. If you have not yet chosen any destination computers, this list will be blank.

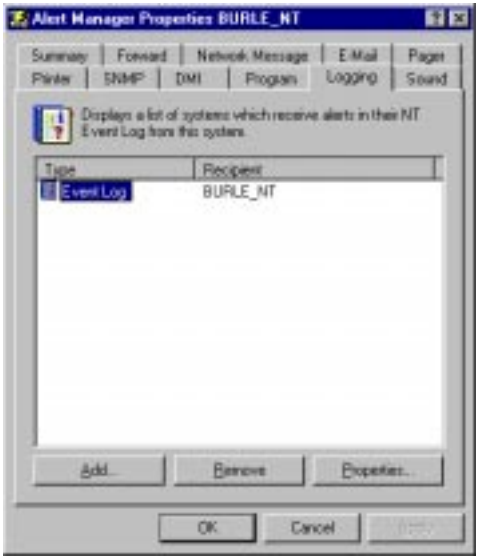


Figure 7-21. Alert Manager Properties dialog box (Logging page)

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 Logging dialog box (Figure 7-7), then enter the name of 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.

     The Windows NT Event Log service must be enabled on the computers you select. To view the status of the Event Log service, open the Windows NT Services from the Control Panel and select EventLog. Click the Startup button and select the Automatic option to start the Event Log service every time the system starts.

     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 Logging Properties dialog box (Figure 7-22). 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. Enter the computer to receive network messages or click Browse to locate the computer.

Figure 7-22. 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 74), 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 Network Message Properties dialog box.

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

   The message will appear instantly on the destination computer's Event Log.

6. Click OK to return to the Alert Manager Properties dialog box.

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

Using Centralized Alerting

Centralized Alerting is a powerful feature for alerting the appropriate personnel of workstation virus activity. Once Centralized Alerting is enabled and configured, workstations using Network Associates client antivirus software, such as VirusScan, report virus activity to NetShield servers. NetShield then notifies the appropriate personnel (through pagers, printers, e-mail, fax, etc.) listed in the Alert Manager Summary property page. To configure Alert Manager, see "Using Alert Manager" on page 69.

How Centralized Alerting works

The NetShield server is configured to monitor an Alert Folder where all users have create, write, and delete rights. When a virus event occurs on a workstation, the workstation sends a Centralized Alerting file to the server's Alert Folder. The server then reads the file and notifies the appropriate personnel specified in Alert Manager.

For information on the Centralized Alerting file format, see "Centralized Alerting .ALR File Format" on page 184.

Configuring Centralized Alerting

To configure Centralized Alerting, follow these steps:

1. Select Alerts from the Tools menu.

   Response: The Alert Properties window is displayed (Figure 7-1 on page 69).

2. Select Enable Centralized Alerting.

   ✍ *Centralized Alerting is enabled by default.*

3. Enter the location of the Alert Folder in the text box provided. You can click Browse to locate the Alert folder on the network.

   ✍ *The default Alert folder is located in C:\Program\Mcafee\NetShield\Alert.*

4. All users must have create, write, and delete rights to the Alert Folder.

5. Click OK.

6. Configure the desktop machines which will report virus activity. For more information, refer to the documentation which accompanied VirusScan.

Customizing Alerts

Enabling/disabling alerts

To enable and disable alerts, complete the following procedure.

Step	Action

1. Select Alerts from the Tools menu and click the Messages tab.

   Response: The Alert properties sheet appears with the Messages page displayed (Figure 7-23).

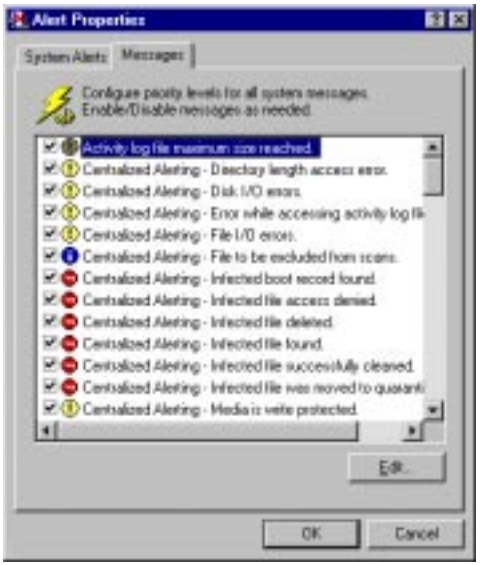


Figure 7-23. Alert Properties dialog box (Messages page)

2. To enable an alert, select its checkbox.

3. To disable an alert, deselect its checkbox.

4. To save the changes and exit, click OK. To exit without saving changes, click Cancel.

Changing the priority of an alert

To change the priority level of an alert, follow these steps:

1. Select Alerts from the Tools menu and click the Messages tab.

   Response: The Alert properties sheet appears (Figure 7-23) with the Messages page displayed.

2. Highlight an alert and click Edit.

   Response: The Configure System Message dialog box is displayed (Figure 7-24).

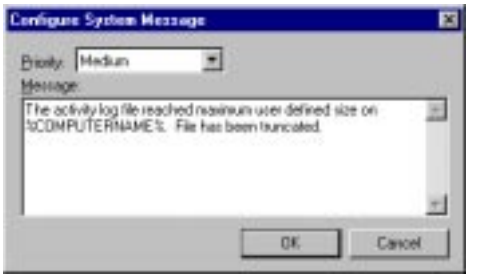


Figure 7-24. Configure System Message dialog box

3. Select a priority level.

4. Click OK.

Customizing an alert message

To customize an alert message, follow these steps:

✍ *While an alert message can be customized, the reason for the alert does not change (e.g. when a task starts, the 'task has started' message is generated). Be careful not to modify the meaning of the alert message. Otherwise, notifications may become confusing or erroneous.*

1. Select Alerts from the Tools menu and click the Messages tab.

   Response: The Alert properties sheet appears (Figure 7-23) with the Messages page displayed.

2. Highlight an alert and click Edit.

   Response: The Configure System Message dialog box is displayed (Figure 7-24).

3. Enter a custom message in the text field.

4. Click OK.

Alert Message variables

Alert messages generated by NetShield may contain following variables:

- %FILENAME% - Name of the infected file
- %TASKNAME% - Name of the task that detected the virus
- %VIRUSNAME% - Name of the virus
- %DATE% - Date of the event
- %TIME% - Time of the event
- %COMPUTERNAME% - Name of the infected computer
- %SOTWARENAME% - Name of the software that detected the virus
- %SOFTWAREVERSION% -Version number of the software that detected the virus
- %USERNAME% -Name of the local user

8 Updating NetShield

Overview

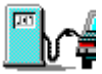
New viruses are discovered at a rate of more than 200 a month. Often, these viruses are not detected using older versions of virus detection products or virus signature (.DAT) files. The .DAT files that came with your copy of NetShield may not detect a virus that was discovered after you bought the product. As new viruses are discovered, Network Associates updates these .DAT.DAT files to detect new viruses on a monthly basis. Network Associates recommends that you update your .DAT files and product on a regular basis to prevent infection from new viruses.

To update your NetShield files, download the updates and apply them to your current NetShield files. There are two ways you can update your NetShield files: automatically or manually.

You can update NetShield automatically by using the AutoUpdate utility or SecureCast service. Both updating services conveniently deliver the latest product upgrades and .DAT file updates to your desktop. For more information about AutoUpdate, see “Using AutoUpdate” on page 104. For information about acquiring the SecureCast software and using its services, see “Updating Your Software Using SecureCast” on page 133.

To perform a manual update, see “Updating your .DAT files manually” on page 115.

Using AutoUpdate



Network Associates' AutoUpdate program is a powerful updating utility that can ensure you have the latest NetShield files installed. AutoUpdate can automatically retrieve the latest NetShield files from Network Associates' FTP site or a local network computer and overwrite old NetShield files on your network. Use the AutoUpdate tasks to automate and customize the updating process.

Network Associates offers two AutoUpdate tasks to keep your NetShield files up-to-date:

- Automatic .DAT Update
- Automatic Product Upgrade

Network Associates updates NetShield virus signature (.DAT) files approximately once a month with new virus detectors, cleaners, and fixes to reported bugs. For information about configuring the Automatic .DAT Update task, see "Automatic .DAT Update task" on page 105. Network Associates upgrades the NetShield program periodically with new features, enhancements, and functionality to provide you with the latest antivirus technology. For information about configuring the Automatic Product Upgrade task, see "Automatic Product Upgrade task" on page 109.

Both AutoUpdate tasks appear in the AntiVirus Console task window preceded by  .

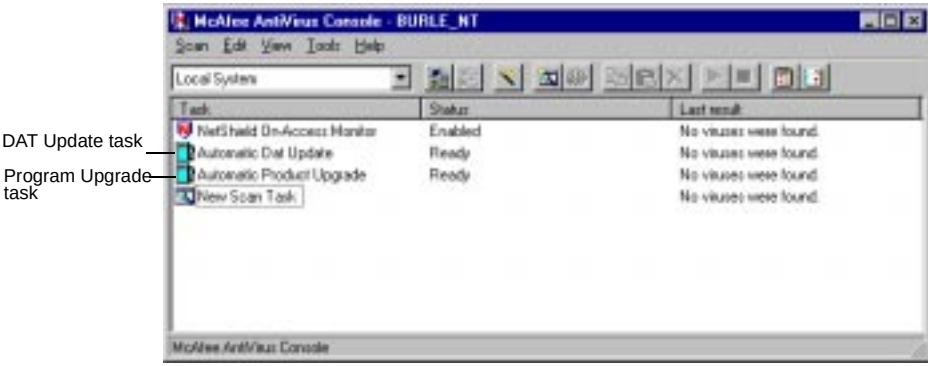


Figure 8-1. AntiVirus Console

Automatic .DAT Update task

How Automatic .DAT Update works

The Automatic .DAT Update task automatically connects to the Network Associates FTP site or a local network computer, and seeks out the latest .DAT file. Then downloads the .DAT files, extracts and inspects them to ensure that all update files are present.

✍ *The Update task looks for the .DAT files in their original .ZIP image. Do not extract the .ZIP file or rename it (e.g. November 1997 .DAT file is called dat-3011.zip).*

When all of the update files are verified, AutoUpdate begins to overwrite the old version of .DAT files with the new version. AutoUpdate then backs up the existing .DAT files and starts the .DAT reload process to complete the update.

Updating .DAT files

To configure the .DAT Update task to acquire and install the latest .DAT files, follow these steps:

Step	Action
1.	Select AutoUpdate from the Tools menu. **Response**: The AutoUpdate properties dialog box appears with the Update Options property page displayed (Figure 8-2).

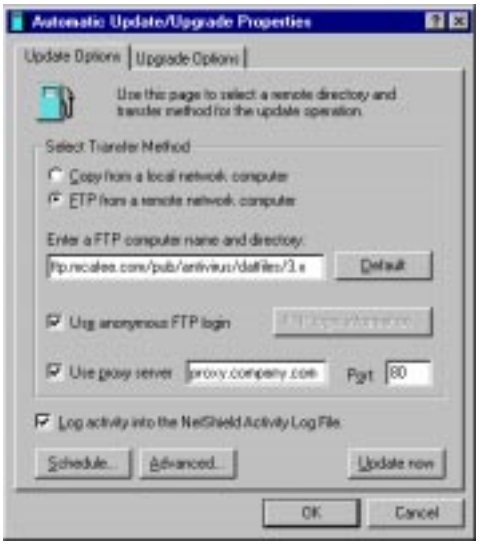


Figure 8-2. AutoUpdate Properties dialog box (Update Options page)

2. Select the transfer method in which you want to receive the files. Your options are:

- **Copy from Local Network Computer.** Choose this option to copy files from a designated computer on your network. Then enter the name of the computer that AutoUpdate will copy the files from 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.

- **FTP from a Remote Network computer.** Choose this option to download files from a designated network computer. Then Enter the FTP computer name and directory in which the files will be downloaded from.

  ✍ *The default FTP computer name and directory is ftp.web.mcafee.com/pub/antivirus/datafiles/3.x*

3. Click the FTP Login Information button to enter your FTP access information, such as username and password, or select the Use Anonymous FTP Login checkbox. If this option is selected, AutoUpdate will automatically assign “Anonymous” as your user name and assign your e-mail address as your password.

   ✍ *Use anonymous FTP login when connecting to Network Associates’ FTP site.*

4. Select the Use Proxy Server checkbox if your environment requires that you use a proxy server to access the Internet via FTP. Enter the name and port number of the proxy server. If you are unsure if your network uses a proxy server or if you do not know the port number, check with your system administrator.

5. Select the Log Activity into the NetShield Activity Log File checkbox to record the AutoUpdate history. The NetShield Activity Log File lists the each step made by AutoUpdate during the updating process. The log file will also include a specific error message if any of these steps fail.

6. To update the .DAT files immediately (on-demand), click the Update Now button.

   Response: AutoUpdate starts to download the latest .DAT file. A status dialog box appears and displays progress messages similar to the log file entries listed on page 87.

   When the “Update of .DAT file is successful” message appears, your NetShield .DAT files are now up-to-date. If an update is not required at this time or the network/FTP connection is interrupted, an error message appears in the status dialog box. Click OK to close the status dialog box. Then view the system event log to get more information about the error.

7. To perform scheduled .DAT file updates, click the Schedule button. See “Advanced Upgrade options” on page 112 for details.

8. Click the Advanced button to configure AutoUpdate to perform special actions during or after the updating process. See the next section for details.

Advanced Update options

The Automatic .DAT Update tasks and can also perform services during and after the updating process. This task can backup existing .DAT files, save the new file for later use, and run a program upon performing the task. To configure the Advanced options, follow these steps:

Step	Action

1. Click the Advance button in the Update Options property page.

   Response: The Advance Update Options dialog box appears (Figure 8-3).

Figure 8-3. Advanced Update Options dialog box

2. Select the Backup the Existing .DAT Files checkbox to automatically backup the existing files.

3. Select the Retrieve the Update File But do Not Perform the Update checkbox to save new .DAT files on the NetShield server without applying them. Enable this option on the local network computer that other NetShield servers and workstations will copy the updates from.

   ✍ *If this option is selected, you must select the Save the Update for Later Use checkbox, then save the file to a location in which it can be retrieved by other NetShield servers and workstations.*

4. Select the Save the Update File for Later Use checkbox to save the new .DAT files in special location. Enter a location in which you want to store the update.

   ✍ *If other NetShield servers are configured to copy the updates from this location, ensure they have appropriate rights.*

5. Check the Run a Program After a Successful Update checkbox to automatically execute a program or script upon downloading the update. Enter the complete path to the file that will be run or click Browse to navigate to the program.

6. Click OK.

Automatic Product Upgrade task

How Automatic Product Upgrade works

The Automatic Product Upgrade task automatically connects to an FTP site or a local network computer, and seeks out the latest version of NetShield. Then downloads the .DAT files, extracts and inspects them to ensure that all update files are present.

✍ *The Upgrade task looks for an unzipped image of the product. This enables administrators to customize the install prior to deploying it.*

When all of the upgrade files are verified, AutoUpdate begins to overwrite the old NetShield files with the new version. AutoUpdate then backs up the existing files and starts the product reload process to complete the update.

Upgrading NetShield

To configure the Product Upgrade task to acquire and install the most current NetShield files, follow these steps:

Step	Action

1. Select AutoUpdate from the Tools menu. Then click the Upgrade tab.

   Response: The AutoUpdate properties dialog box appears with the Upgrade Options property page selected (Figure 8-4).

Figure 8-4. AutoUpdate Properties dialog box (Upgrade Options page)

2. Select the transfer method in which you want to receive the files. Your options are:

   - **Copy from Local Network Computer.** Choose this option to copy files from a designated computer on your network. Then enter the name of the computer that AutoUpdate will copy the files from 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.

- **FTP from a Remote Network computer.** Choose this option to download files from a designated network computer. Then Enter the FTP computer name and directory in which the files will be downloaded from.

3. Click the FTP Login Information button to enter your FTP access information, such as username and password, or select the Use Anonymous FTP Login checkbox. If this option is selected, AutoUpdate will automatically assign “Anonymous” as your user name and assign your e-mail address as your password.

4. Select the Use Proxy Server checkbox if your environment requires that you use a proxy server to access the Internet via FTP. Enter the name and port number of the proxy server. If you are unsure if your network uses a proxy server or if you do not know the port number, check with your system administrator.

5. Select the Log Activity into the NetShield Activity Log File checkbox to record the AutoUpdate history. The NetShield Activity Log File lists the each step made by AutoUpdate during the updating process. The log file will also include a specific error message if any of these steps fail.

6. To upgrade NetShield immediately (on-demand), click the Update Now button.

   Response: AutoUpdate starts to download the latest NetShield program. A status dialog box appears and displays progress messages similar to the log file entries listed on page 87.

   When the “Upgrade of NetShield is successful” message appears, NetShield is now upgraded. If an upgrade is not required at this time or the network/FTP connection is interrupted, an error message appears in the status dialog box. Click OK to close the status dialog box. Then view the system event log to get more information about the error.

7. To perform scheduled product upgrades, click the Schedule button. See “Advanced Upgrade options” on page 112 for details.

8. Click the Advanced button to configure AutoUpdate to perform special actions during or after the updating process. See the next section for details.

Advanced Upgrade options

The Automatic Product Upgrade task can also perform services during and after the updating process. This task can backup existing NetShield files, save the new files for later use, and run a program upon performing the upgrade. To configure the Advanced options, follow these steps:

Step	Action

1. Select AutoUpdate from the Tools menu. Then click the Upgrade tab.

   Response: The AutoUpdate properties dialog box appears with the Upgrade Options property page selected (Figure 8-4).

2. Click the Advance button in the Upgrade Options property page.

   Response: The Advance Update Options dialog box appears (Figure 8-3).

Figure 8-5. Advanced Update Options dialog box

3. Select the Retrieve the Upgrade Files But do Not Perform the Upgrade checkbox to save new files on the NetShield server without applying them. Enable this option on the local network computer that other NetShield servers and workstations will copy the updates from.

   ✍ *If this option is selected, you must select the Save the Upgrade Files for Later Usage checkbox and specify the location in which the file can be retrieved.*

4. Select the Save the Update File for Later Use checkbox to save the new files without applying them. Enter a location in which you want to store the files in the text box provided. You can enter the location in Universal Naming Convention (UNC) notation, or you can click Browse to locate the location on the network.

   ✍ *If other NetShield servers are configured to copy the upgrade files from this location, ensure they have appropriate rights.*

5. Click OK.

Scheduling AutoUpdate tasks

Scheduling allows you to update .DAT files or upgrade NetShield automatically at any time you choose. The AutoUpdate tasks can be scheduled to run once, daily, weekly, monthly, hourly, or each time the service is started.

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

Step	Action

1. Select the Enable Scheduler checkbox.

   ✍ *If the Scheduler is not enabled, NetShield will not receive updates or upgrades automatically.*

2. Determine how often downloading should occur. Choose from these options:

   - **Once.** This tells AutoUpdate to perform a one time update or upgrade at the time and .DATe you specify. Enter the time and .DATe downloading will occur.
   - **Hourly.** This tells AutoUpdate to download NetShield files at the hour you specify.
   - **Daily.** This tells AutoUpdate to download NetShield files only on the days you specify.
   - **Weekly.** This tells AutoUpdate to download NetShield files once a week.
   - **Monthly.** This tells AutoUpdate to download NetShield files once a month.
   - **At Startup.** This tells AutoUpdate to download NetShield files every time the service is started.

3. Click OK.

Updating your .DAT files manually

To update your Network Associates .DAT files manually, without using AutoUpdate, follow these steps:

Step	Action
1.	Download the .DAT file (for example, .DAT-3011.ZIP) from one of Network Associates' electronic services. On most services, it is located in the anti-virus area.
2.	Copy the file to a new directory.
3.	The file is in a compressed format. Decompress the file using any PKUNZIP-compatible decompression software. If you don't have the decompression software, you can download PKUNZIP (shareware) from Network Associates electronic sites.
4.	Locate the directories on the hard drive where NetShield is currently installed. Typically, the files are stored in C:\Program Files\McAfee\NetShield.
5.	Back up the existing .DAT files to a different directory, then copy the new files into the appropriate directory or directories, overwriting the old .DAT files. ✍ *There might be part of the software in more than one directory. If so, place each updated file in the appropriate directory.*
6.	Stop and restart the NetShield Task Manager for the changes to take effect.

Validating the NetShield program files

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

A Encountering Viruses

Removing Viruses

NetShield and VirusScan offer a variety of cleaning options. If NetShield or VirusScan prompts you to remove a virus, follow these steps:

1. Select how to respond to the virus infection. Choose from these options:

   - **Clean.** Choose this options to clean the file or remove the virus from the file.
   - **Delete.** Choose this option to delete the file.

     ✍ *Note the filename and path to restore the file from backups. To configure NetShield or VirusScan to automatically keep track of deleted files, select the Log To File option. See* *"Creating a virus activity log" on page 44*.

   - **Move File To.** Choose this option to move the infected file to a quarantine folder.
   - **Continue.** Choose this option to continue scanning without taking any action.

     ✍ *This option is not recommended.*

2. Repeat the previous step until all viruses are found and removed.

   ✍ *If NetShield or VirusScan cannot clean a virus, run VirusScan or NetShield again, delete the infected files, and restore them from backups.*

3. To configure NetShield to automatically clean, delete, or move infected files in the future, see “Setting how NetShield responds to a virus infection” on page 38.

4. To find and eliminate the source of the infection, scan your diskettes immediately.

When NetShield detects a virus in a file, it will take the action specified during configuration. See “Responding to infections” on page 45 (on-access scanning) or “Setting NetShield’s response to a virus infection” on page 58 (on-demand scanning).

If you selected Clean Infected Files

If you selected Clean Infected Files from the Action property page and a virus is found, NetShield will automatically attempt to clean the file.

To confirm the virus was cleaned, check the NetShield Log File. If the virus was not successfully removed, delete the file and restore it from backups.

If you selected Delete Infected Files

If you selected Delete Infected Files from the Action property page and a virus is found, NetShield will automatically delete the infected file.

If this option is selected, confirm that report logging is enabled. This will ensure you have a record of which files were deleted, so you can restore them from backups. See “Logging on-access scan activity” on page 48 (on-access scanning) and “Logging on-demand scans” on page 61 (on-demand scanning).

If NetShield is unable to delete an infected file, confirm the file is not write-protected.

If you selected Move Infected Files

If you selected Move Infected Files from the Action property page and a virus is found, the infected file will automatically be moved to the specified directory.

After the file is moved to the quarantine directory, you can clean the file or restore the file from backups and return it to its original location. To help you locate the source of the infection, the path to infected file is duplicated in the quarantine directory. For example, if an infected file was found in SYS:USERS\JOE and you specified SYS:INFECTED as the quarantine directory, it would be copied to SYS:INFECTED\USERS\JOE.

If you selected Continue Scanning

If you selected Continue Scanning from the Action property page and a virus is found, NetShield will continue scanning without taking any action.

✍ *This option is not recommended for most applications. If you do use this option, make sure report logging is enabled. See "Logging on-access scan activity" on page 48 for on-access scanning or "Logging on-demand scans" on page 61 for on-demand scanning.*

B

Using VirusScan

What is VirusScan?

VirusScan is an independent desktop program that complements the NetShield Console. The NetShield Console automates the process of scanning and is ideal for implementing long-term anti-virus strategies. VirusScan offers a quick way to scan for viruses.

Use the VirusScan properties sheet to configure scan settings. To open the VirusScan properties sheet, do one of the following:

- In Windows NT 3.51, open the NetShield group in the Windows NT Program Manager and double-click the VirusScan icon, or
- In Windows NT 4.0, click Start, select NetShield in the Programs menu, and select VirusScan.

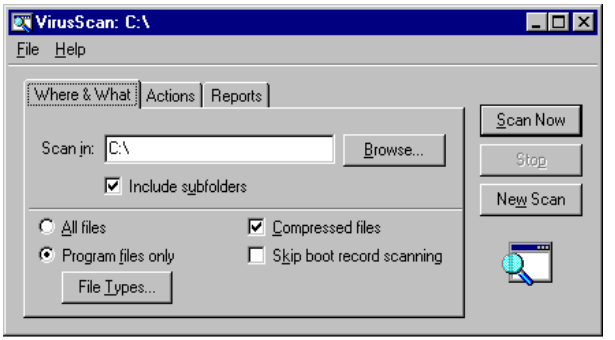


Figure B-1. VirusScan dialog box (Where & What property page)

Using VirusScan

Configuring scan options

Use the Where & What property page to specify which files VirusScan should scan for viruses.

To scan for viruses using VirusScan, follow these steps:

1. Enter a location to scan or click Browse to choose a location.
2. To include scanning of subfolders, select the Include Subfolders checkbox.
3. Select the types of files to scan:
   - **All Files**. This tells VirusScan to scan every file type. This option is your best protection against infection.
   - **Program Files Only**. This tells VirusScan to scan only the files that are most susceptible to virus infection. Click the File Types button to specify the filename extensions that VirusScan uses to identify these files.

     Response: The Program File Extensions dialog box appears (Figure B-2).

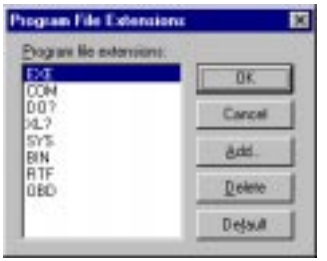


Figure B-2. Program File Extensions dialog box

✍ *By default, NetShield identifies files with the extensions .EXE, .COM, .DO?, .XL?, .SYS, .BIN, .RTF, and .ODB as most susceptible to virus infection. It uses the extensions .DO?, and .XL? to identify Microsoft Word and Excel document and template files, which can contain macro viruses. The ? character is a wildcard.*

- To add a file extension, click Add. Enter a new file extension to scan and click OK. Repeat this procedure until all desired file extensions are entered.
- To delete an extension, highlight it and click Delete.
- To return to the default extensions, click Default.

When you are finished editing the list of file extensions, click OK.

4. Select the Compressed Files checkbox to scan files compressed with PKZIP, LHA, LZH, WinZip, PKLITE, LZEXE, or Microsoft CAB.

5. Select the Skip Boot Record Scanning checkbox to skip the scanning of the system's boot record.

6. Click the Scan Now button to initiate the scan or choose another property page to further configure this scan.

Responding to infections

Use the Actions property page to tell VirusScan what to do when it finds a virus.

1. Select a response from the When a Virus is Found pull-down list. Your choices are:

- **Continue Scanning.** Use this option to ignore infected files and continue scanning. VirusScan will not take any action when it detects a virus.
- **Prompt for Action.** Use this option if the computer will be attended when the scan is running. VirusScan will ask the user what to do with each virus as it is found.
- **Move infected files to a folder.** Use this option to tell VirusScan to move infected files to a "quarantine" directory. Specify a path in the Folder To Move To box or choose Browse to locate a folder.

- **Clean infected file.**

  ✍ *If a virus cannot be removed from a file or the file is damaged beyond repair, VirusScan automatically denies access to the file. If this occurs, delete the file and restore the original from backups.*

- **Delete infected file.** Use this option to tell VirusScan to delete infected files as soon as it detects them.

  ✍ *If you select automatic deletion of infected files, make sure to select the Log To File checkbox. When VirusScan finishes deleting infected files, you can look them up in the log file and restore them from backups.*

2. Click the Scan Now button to initiate the scan or choose another property page to further configure this scan.

Reporting options

Use the Reports property page to configure VirusScan's reporting options.

1. Select the Display Custom Message checkbox to display a custom message. Enter a message in the space provided.

   ✍ *For VirusScan to display a custom message, the Prompt for Action option must be selected on the Action page.*

2. Select the Notify Alert Manager checkbox to send virus notifications to Alert Manager. See "Using Alert Manager" on page 69 for information about configuring Alert Manager settings.

3. To record scanning information, select the Log To File checkbox. Enter a name and location for the log file or click Browse to choose a location.

   ✍ *VirusScan's default logfile is SCANLOG.TXT.*

Select the Limit Size of Logfile checkbox to keep the logfile from using excessive hard disk space. Specify a size between 10KB and 99999KB. By default, VirusScan sets a limit of 100KB.

4. Click the Scan Now button to initiate the scan or choose another property page to further configure this scan.

C

Network Associates Support Services

Network Associates is pleased to offer many different types of technical assistance to customers. These flexible support programs are designed to meet the needs of individuals and businesses at any level. By offering support solutions that range from a complimentary 90-day introductory technical support program to an optional one-year personal support plan, Network Associates helps to ensure that you receive the level of technical assistance you require.

Network Associates also offers a variety of technical assistance plans designed to meet the needs of business customers, including training, consulting, enterprise support, and a Jump Start program. Please review each of the different support service plans and benefits listed in this appendix and pick the one best suited for you.

✍ *The term update refers only to the virus definition files; the term upgrade refers to product version revisions, executables, and definition files. Network Associates offers free online virus signature file updates (.DATs) for the life of your product. However, we cannot guarantee backward compatibility of the signature files with previous versions' executable files (.EXEs). By upgrading your software to the latest product version and updating to the latest .DAT files regularly, you ensure complete virus protection for the term of your software subscription or maintenance plan.*

Customer Service Programs

Free 90-day introductory support program

All registered owners of single-node products are entitled to online virus updates (new .DAT files), one free online product upgrade (product version revision) with the newest features and virus protection (if applicable), and the free support services listed below during the first 90 days of software ownership.

- Electronic and online support available 24 hours a day, seven days a week on each of the forums listed below:
  - Automated voice and fax system: (408) 988-3034
  - Network Associates BBS (electronic bulletin board system): (408) 988-4004
  - World Wide Web site: http://www.nai.com
  - CompuServe: GO MCAFEE
  - America Online keyword: MCAFEE
- Technical support phone assistance during regular business hours, 6:00 A.M.– 6:00 P.M. Pacific time, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.

To receive your free one-time online upgrade please contact our Sales Support department at (408) 988-3832. Please supply your proof of purchase when you request the upgrade. You will be given a password to the upgrade area on either the Network Associates BBS, FTP site, or World Wide Web site so that you can download a registered version of the latest product. This password is valid for one access only.

Subscription maintenance and support program

Network Associates offers all registered owners of licensed multiple-node subscription products the following free support services and maintenance during the two-year term of the software subscription:

- Electronic and online support available 24 hours a day, seven days a week on each of the forums listed below:
  - Automated voice and fax system: (408) 988-3034
  - Network Associates BBS (electronic bulletin board system): (408) 988-4004
  - World Wide Web site: http://www.nai.com
  - CompuServe: GO MCAFEE
  - America Online keyword: MCAFEE
- Technical support phone assistance during regular business hours, 6:00 A.M.–6:00 P.M. Pacific time, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.
- Two years of free online product upgrades with the newest features and virus protection (if applicable). If you upgrade your operating system, you can also upgrade your Network Associates product to the new platform (for example, from Windows 3.1 to Windows 95).

Optional support plans

✍ *Contact Network Associates for current pricing structures.*

Option 1—one-year personal online maintenance and support program

For registered owners of single-node products who want to extend their support coverage, this plan allows you to call in for unlimited technical support, download the latest virus protections updates each month, and periodically download upgrades from any of Network Associates' registered online services—all for a full year. If you upgrade your operating system, you can also upgrade your product program to the new platform.

Option 2—one-year quarterly disk/CD maintenance and support programs

This plan is for registered owners of either single- or multiple-node subscription products. It offers all the features of Option 1, while adding a quarterly mailing of software upgrade diskettes or CDs (depending on the product) and a quarterly update newsletter. With this option, you can update your product to include the latest features and virus updates without having to download files from an online service.

Each optional support plan begins as soon as you purchase the product and is good for one year, at which time you can renew your support program through Network Associates' Sales Support department at (408) 988-3832.

✍ *Network Associates reserves the right to change part or all of its customer service programs at any time without notice.*

Professional Services Programs

Network Associates Professional Services provide a wide range of on-site services. Whether for short-term assistance or long-term strategic planning, a highly qualified consultant can help you achieve positive results. Network Associates consultants are trained on NetWare, Microsoft NT Advanced Server, Windows 95, and a multitude of desktop applications.

Before work begins, a project manager discusses the project scope and objective with you and comes to a mutual agreement on the job objective. When the consultant leaves the site, you can be sure that the objective has been achieved. For current prices, contact Network Associates.

✍ *Network Associates reserves the right to change part of all of its professional services program at any time without notice.*

Training

Network Associates' expertise and experience is available to your personnel, allowing an organization to take full advantage of computing resources. Network Associates offers on-site training on all Network Associates products, network management seminars, anti-virus seminars, customized curriculums for site-specific applications as well as product and personnel certification. Network Associates' consultants provide extensive training with curriculum tailored to your organization's needs.

Consulting

Network Associates Professional Services offer a number of hourly and daily consulting services including:

- Troubleshooting an existing installation
- Writing PowerScript or SaberBASIC scripts
- Planning and designing networks
- Installation and configuration
- Windows 95 configuration
- One-on-one consulting

Network Associates Professional Services are available on a quotable time and materials basis to perform project management, product research, and a number of other consulting services.

Jump Start program

This fixed-fee consulting program is designed to get clients up and running on Network Associates products as soon as possible. It includes training, installation, and configuration services as needed on a single server. It is designed to demonstrate how to connect various PCs to the LAN, train administrators how to use the program, and master the roll-out process.

Enterprise support

Network Associates' Enterprise Support Program provides customers with the highest level of support possible. This fee-based program is designed for those customers who need a higher level of personal service.

The Enterprise Support Program offers the following features:

- Direct pager number to your assigned senior Enterprise Support Program analyst
- Extended support hours: 7:00 A.M. to 7:00 P.M. central time, Monday through Friday
- Five designated Network Associates contacts
- Proactive support, providing updated company and product information as it becomes available
- On-site services at a 25% discount
- VIP issues review list
- Beta site (if desired)

Each Enterprise Support Representative calls clients each week. This phone call is used to forward any information such as technical notes and application anomalies of which you should be aware. This call also ensures that you have no unresolved problems or complications with the product. Enterprise Support representatives will return your page on the day it is received.

Optional enterprise support feature

7 X 24 support

Frequently, customers are responsible for their own LANs, which run 24 hours a day, seven days a week. This feature offers round-the-clock support for clients requiring support outside normal business hours.

D Updating Your Software Using SecureCast

Introducing SecureCast

Network Associates' SecureCast service conveniently delivers the latest product upgrades and data file updates to your desktop. With it, you can choose to receive updates for your licensed Network Associates software via the Internet, regularly and automatically. To use this option, you must install the SecureCast client software and subscribe to either the Home SecureCast channel (for retail customers) or the Enterprise SecureCast channel (for corporate customers).

If you are a retail customer and would rather decide when to update your system, an option allows you to download new files only when your software reminds you that it's time to update. If you are a corporate customer (but not an administrator), contact your administrator to learn where to update your files, or use the AutoUpdate feature if your product includes it.

Please choose one of the update options listed in this appendix to keep your system efficiently protected from the network to the desktop. With SecureCast, you'll get the latest data files and program files as soon as they're available. New viruses and other harmful agents appear at a rate of more than 200 per month—don't risk letting your data disintegrate or your network become inaccessible simply because you forgot to update or upgrade your software.

✍ *The term* "update" *refers to data (.DAT) files; the term* "upgrade" *refers to product version revisions, executables, and data 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. By upgrading your software to the latest product version and updating to the latest .DAT files regularly via SecureCast, you ensure complete protection for the term of your software subscription or maintenance plan.*

Why would I need to update my data files?

To offer you the best protection possible, Network Associates continually updates data files that detect new viruses and other harmful agents. Although your software has technology that allows it to detect previously unknown strains of viruses or malicious code, new virus types and other agents appear frequently. Often, your existing software cannot detect these intruders because the data files that came with it became outdated. Your software periodically notifies you to update these files. For maximum protection, Network Associates strongly recommends that you update your files on a regular basis.

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 the common .DAT files above, you may also receive some of these additional files, depending on which anti-virus or security products you're running:

- WEBSCANX.DAT or INTERNET.DAT—includes detection string data for hostile Java applets and ActiveX controls. WebShieldX and WebScanX 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.

System requirements

- Windows 95 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 6–65MB per download.
- An active Internet connection—direct or dialup—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 and using your Internet connection when it's idle. You can also 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. New .DAT files are usually available mid-month.
- Alerts on newly identified dangerous viruses.
- Announcements of new versions of software and associated products.

Home SecureCast Channel

Retail customers may install SecureCast client software from a Network Associates CD-ROM.

Understanding SecureCast

If you are a retail customer, you can use SecureCast's timely, free delivery service in one of two ways:

- To receive automatic downloads of the latest updates for your licensed Network Associates software via the Internet, install the SecureCast client, then subscribe to the Home SecureCast channel.

  OR

- If you would rather decide when to update your software, use the included update utility when your software reminds you that it's time.

Downloading automatically

Setting up Home SecureCast

Follow these steps to subscribe to the Home SecureCast channel:

Step	Action
1.	Install the BackWeb client software from a Network Associates CD-ROM. **Response**: You will receive a Welcome InfoPak that tells you that your connection to the Home SecureCast channel is working. An InfoPak can contain sounds, animations, Web pages, and more. When you receive a new InfoPak from Home SecureCast, it will automatically appear as an animated object on your desktop until you open it. To open an InfoPak, simply double-click it.

2. Complete the channel registration process via the User Registration Information dialog box (which will appear in either the first or second InfoPak you receive), then click Next.

   Response: The Online Activity Status dialog box tracks the status of your data transmission.

3. When your user registration is complete, make a note of your registration number, then click Finish.

Using Home SecureCast

You are now ready to receive periodic Virus Alerts, plus product updates and upgrades. Within a few days, you should receive additional InfoPaks. Double-click these to extract and set up the updates or upgrades they contain.

Unsubscribing from Home SecureCast

Follow these steps to cancel this service at any time:

Step	Action

1. Double-click the SecureCast client icon in the Windows taskbar status area.

2. Right-click the Home channel button.

   Response: A shortcut menu appears.

3. Click Unsubscribe, then click OK to confirm.

Initiating a Download

Updating registered software

Network Associates software includes a feature that periodically reminds you to update your software. If many months have passed since you first installed your software, Network Associates strongly recommends that you use the update options described in the following steps to ensure that you are using the latest data files and product versions available.

Updating after installation

After you install your anti-virus or security software, the Welcome dialog box (Figure D-1) prompts you to update your software. This dialog box also appears when you start a computer system pre-loaded with Network Associates software for the fifth time. VirusScan, for example, displays this notice:

Figure D-1. Welcome dialog box

1. Click Update to receive the latest version of the software for free.

   Response: The Internet Access dialog box (Figure D-2) appears.

Figure D-2. Internet Access dialog box

2. If you have Internet access, select Yes, then click Next. If you do not have Internet access, select No, then click Next.

Response: The Server dialog box (Figure D-3) appears. If you selected Yes, then the dialup-number box will be unavailable; if you selected No, then the dialup-number box will be available.

Figure D-3. Server dialog box

3. If you have Internet access, verify your Country Code and Area Code, and click Next. If you don't have Internet access, verify your Country Code and Area Code, select a modem dialup number, and click Next.

Response: Your system connects to a Network Associates server.

- If the server has no new .DAT file updates or software upgrades, the Online Activity Status dialog box (Figure D-4) tells you that your files are up-to-date.

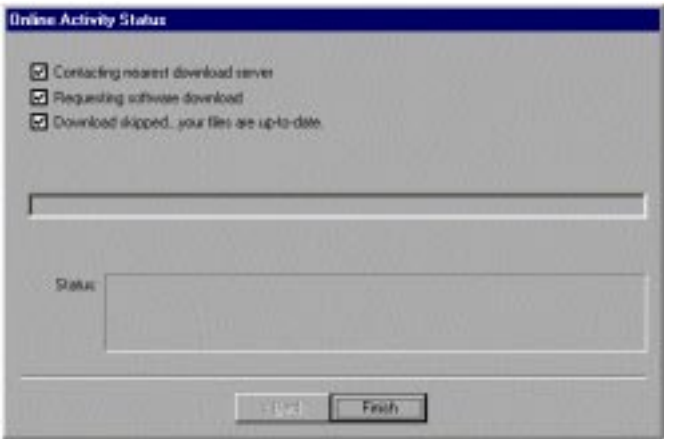


Figure D-4. Online Activity Status dialog box (No Download)

  - Click Finish to disconnect from the server.

- If the server has new .DAT files, the Online Activity Status dialog box (Figure D-5) tells you that the .EXE file containing the .DAT files is automatically downloading to your system.

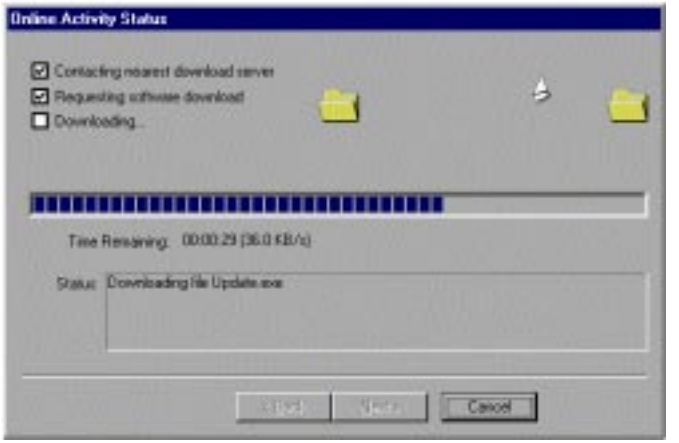


Figure D-5. Online Activity Status dialog box

- When the download is complete, click Next. The Online Activity Complete dialog box (Figure D-6) appears.

Figure D-6. Online Activity Complete dialog box

- Click Finish to install your new .DAT file updates.

- If the server has a product version more recent than yours, the Newer Component Found dialog box (Figure D-7) appears. To download only the latest .DAT files, select .DAT files only, then click Next. To download a new product version, click Next.

Figure D-7. Newer Component Found dialog box

Response: The Online Activity Status dialog box (see Figure D-5 on page 141) tracks the status of your download.

4. When your download is complete, click Next to continue.

Response: The Online Activity Complete dialog box (Figure D-8) confirms that your download is complete.

Figure D-8. Online Activity Complete dialog box

5. Note the name and location of the downloaded file, then click Finish to install your software.

Updating at periodic intervals

At 30-day intervals, the Update dialog box (Figure D-9) prompts you to update your software.

Figure D-9. Update dialog box

If you are a registered user, complete the following steps to receive the latest version of the software for free. Repeat the update process every month when prompted.

✍ *As a registered user, you can continue to receive .DAT file updates for the life of your product. Network Associates cannot, however, guarantee compatibility between future .DAT file updates and older product versions. By purchasing the latest software upgrades via SecureCast, you ensure complete virus protection for the term of your software subscription or maintenance plan.*

1. Click Update to receive the latest version of the software for free.

   Response: The Internet Access dialog box (see Figure D-2 on page 139) appears.

2. If you have Internet access, select Yes, then click Next. If you do not have Internet access, select No, then click Next.

   Response: The Server dialog box (see Figure D-3 on page 139) appears. If you selected Yes, then the dialup-number box will be unavailable; if you selected No, then the dialup-number box will be available.

3. If you have Internet access, verify your Country Code and Area Code, and click Next. If you don't have Internet access, verify your Country Code and Area Code, select a modem dialup number, and click Next.

   Response: Your system connects to a Network Associates server.

   - If the server has no new .DAT file updates or software upgrades, the Online Activity Status dialog box (see Figure D-4 on page 140) tells you that your files are up-to-date.
     - Click Finish to disconnect from the server.
   - If the server has new .DAT files, the Online Activity Status dialog box (see Figure D-5 on page 141) tells you that the .EXE file containing the .DAT files is automatically downloading to your system.
     - When the download is complete, click Next. The Online Activity Complete dialog box (see Figure D-6 on page 141) appears.
     - Click Finish to install your new .DAT file updates.
   - If the server has a product version more recent than yours, the Newer Component Found dialog box (see Figure D-7 on page 142) appears. To download only the latest .DAT files, select .DAT files only, then click Next. To download a new product version, click Next.

   Response: The Online Activity Status dialog box (see Figure D-5 on page 141) tracks the status of your download.

4. When your download is complete, click Next to continue.

Response: The Online Activity Complete dialog box (Figure D-10) confirms that your download is complete.

Figure D-10. Online Activity Complete dialog box

5. Note the name and location of the downloaded file, then click Finish to install your software.

Registering evaluation software

If you are using a 30-day evaluation version of Network Associates software, the Purchase dialog box (Figure D-11) appears. This dialog box also appears when you select Purchase from the File menu of your Network Associates software.

Figure D-11. Purchase dialog box

If you continue to use evaluation copies of Network Associates software after their 30-day licenses expire, you will see increasingly frequent reminders to register your software. Network Associates strongly recommends that you follow these steps to ensure that you are using the newest data files and product versions available:

Step	Action
1.	In the Purchase dialog box (Figure D-11), click Purchase to begin registering your evaluation copy of anti-virus software electronically. **Response**: The Internet Access dialog box (see Figure D-2 on page 139) appears.
2.	If you have Internet access, select Yes, then click Next. If you do not have Internet access, select No, then click Next.

Response: The Server dialog box (see Figure D-3 on page 139) appears. If you selected Yes, then the dialup-number box will be unavailable; if you selected No, then the dialup-number box will be available.

3. If you have Internet access, verify your Country Code and Area Code, and click Next. If you don't have Internet access, verify your Country Code and Area Code, select a modem dialup number, and click Next.

   Response: Your system connects to a Network Associates server.

   - If the server has no new .DAT file updates or software upgrades, the Online Activity Status dialog box (see Figure D-4 on page 140) tells you that your files are up-to-date.
     - Click Finish to disconnect from the server.
   - If the server has new .DAT files, the Online Activity Status dialog box (see Figure D-5 on page 141) tells you that the .EXE file containing the .DAT files is automatically downloading to your system.
     - When the download is complete, click Next. The Online Activity Complete dialog box (see Figure D-6 on page 141) appears.
     - Click Finish to install your new .DAT file updates.
   - If the server has a product version more recent than yours, the Newer Component Found dialog box (see Figure D-7 on page 142) appears. To download only the latest .DAT files, select .DAT files only, then click Next. To download a new product version, complete steps 4 through 9.

4. Click Next to obtain the newer version of the software.

   Response: A second Newer Component Found dialog box (Figure D-12) appears if you are no longer entitled to free software upgrades.

Figure D-12. Newer Component Found dialog box #2

✍ *File sizes and support pricing are dynamically generated, thus may vary from what you see above when you download your purchase.*

5. Click Next to continue the download.

Response: The Enter Credit Card Information dialog box (Figure D-13) appears.

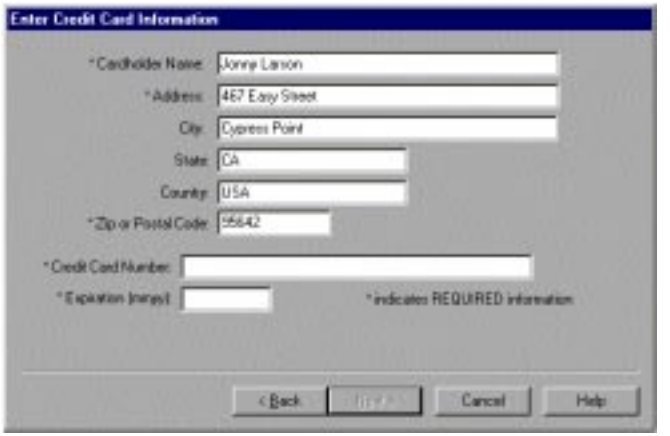


Figure D-13. Enter Credit Card Information dialog box

6. Enter your credit card billing address, account number, and expiration date. Click Next to continue.

   ✍ *Your credit card details are safely transmitted in a secure transaction.*

   Response: The Online Purchase Authorization dialog box (Figure D-14) appears.

Figure D-14. Online Purchase Authorization dialog box

7. Select the check box to authorize the transaction charges to your credit card, and click Click Here to Buy to begin the download process.

   ✍ *Your credit card will not be charged unless you successfully complete the download.*

   Response: The Online Activity Status dialog box (see Figure D-5 on page 141) tracks the status of your download.

8. When your download is complete, note the resulting transaction number for your purchase, then click Next to continue.

   Response: The Online Activity Complete dialog box (see Figure D-8 on page 142) confirms that your transaction is complete.

9. Note the name and location of the downloaded file, then click Finish to install your software.

Enterprise SecureCast Channel

If you manage a corporate network, you may download BackWeb's client software from Network Associates' corporate site (http://www.nai.com) and install it on a network server. Enterprise SecureCast is for use by administrators only, not by corporate end users.

✍ *When the first InfoPak arrives, double-click it to open it, then complete the channel registration process via the Customer Registration Information dialog boxes. When you receive subsequent InfoPak files from Enterprise SecureCast, Network Associates strongly recommends that you distribute them to individual desktops as needed, in order to conserve network bandwidth.*

Benefits

- Ease of use

  You no longer have to search for and download updates from Network Associates' electronic distribution services. The updates you need will be delivered to you in a zipped format, ready for onsite testing and installation.

- Timely protection

  Network Associates provides you with timely protection by regularly delivering .DAT file updates and product upgrades directly to your desktop. As soon as the updates are released to the SecureCast server, they start to transfer to your site.

- Virus Alerts

  You will receive Virus Alerts that notify you of threatening viruses and suggest the best way to prevent infection. In addition, alerts that distinguish between hoaxes and serious threats will save you valuable time and prevent unnecessary concern.

- Upgrades for multiple platforms

  A subscription to Enterprise SecureCast allows you to receive upgrades and updates to your products for multiple platforms. Data file updates and product upgrades for Windows 95, Windows NT, Windows 3.1x, DOS, OS/2, and the Mac OS can be delivered to your desktop.

- Localized language versions

  With your subscription, you receive .DAT file updates not only across multiple platforms, but also in the languages of your choice.

- HTTP support in client software

  Enterprise SecureCast supports HTTP (Hypertext Transfer Protocol) for file transmission through your firewall to the SecureCast servers.

  ✍ *Firewall considerations: If you have a firewall in place, use HTTP. If you do not, use UDP. If you are using Check Point's Firewall-1™ software, you'll notice that BackWeb is a predefined transmission type.*

Setting up Enterprise SecureCast

To obtain the BackWeb client, corporate customers must first have a grant number (product license serial number) to enroll for 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/securecast/esc/grantreq.asp

  OR

  Send an e-mail message to the appropriate address:

  ESCRegistration@cc.nai.com (United States)

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

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

Follow these steps to set up Enterprise SecureCast:

Step	Action
1.	Download the Enterprise SecureCast BackWeb client (about 2MB). This client software is specially configured to function in the corporate environment, supporting HTTP file transmission.
2.	Install the Enterprise SecureCast client software. **Response**: You will receive a Welcome InfoPak that tells you that your connection to the Enterprise SecureCast channel is working.
3.	Begin the channel registration process by entering data about your company in the Customer Registration Information dialog boxes (which will appear in either the first or second InfoPak you receive). **Response**: After you click Next on the last registration dialog box, the Online Activity Status dialog box tracks the status of your data transmission.
4.	When your user registration is complete, make a note of your registration number, then click Finish. **Response**: Your web browser launches showing a product signup form.
5.	Select the software, the platforms, and the languages for which you want to receive upgrades and updates.
6.	Submit your product signup form.

Using Enterprise SecureCast

You are now ready to receive periodic Virus Alerts, plus product updates and upgrades. Within a few days, you should receive additional InfoPaks. An InfoPak can contain sounds, animations, Web pages, and more. When you receive a new InfoPak from Enterprise SecureCast, it will automatically appear as an animated object on your desktop until you open it. To open an InfoPak, simply double-click it.

Once the updates are on your system, you must distribute them to the workstations on your network. The InfoPaks you receive work well as distribution packages for McAfee Enterprise (Me!) With Me!, you can manage software updates, inventory, distribution, usage metering, and centralized alerting. Contact your Network Associates sales representative for more information about Me!

Troubleshooting Enterprise SecureCast

Registration problems

If you try to register during a busy time of day on the Web, you may encounter a delay when 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 for assistance.

Firewall problems

Most firewalls that allow web-browsing traffic will also allow you to receive SecureCast InfoPaks. Some firewalls, however, can cause some problems connecting to the SecureCast server. When you complete the registration form and download the software, you will initially download a SecureCast client built with BackWeb version 1.2. Because version 1.2 does not support certain communication protocols, you might see an error similar to "no network connection" when you use it. To correct this problem, download the latest SecureCast client, which was developed with BackWeb version 3.0.

✍ *You must install the client software that uses BackWeb version 3.0 over the client that uses the 1.2 version of BackWeb. DO NOT uninstall the older version first. This ensures that the new SecureCast client will retain your channel preferences.*

Follow these steps to install and configure the newer SecureCast client software:

Step	Action
1.	Install BackWeb version 3.0 over BackWeb version 1.2.
2.	Start the SecureCast client.
3.	To configure the SecureCast client's Communication Method with your own network information, choose Global Options from the Preferences menu.
4.	Change the setting for how BackWeb navigates through your proxy server from Polite Agent to HTTP. Next, click HTTP Proxy Setup, then enter the requested information about your network. ✍ *Keep in mind that your proxy server information is specific to your network. If you have further questions, consult your system administrator.*

Unsubscribing from Enterprise SecureCast

Follow these steps to cancel this service at any time:

Step	Action
1.	Double-click the SecureCast client icon in the Windows taskbar status area.
2.	Right-click the Enterprise channel button. **Response**: A shortcut menu appears.
3.	Click Unsubscribe, then click OK to confirm.

Support Resources

SecureCast

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

http://www.nai.com/securecast/securefaq.html

BackWeb

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

  http://www.nai.com/securecast/securedetail.html

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

  http://www.backweb.com/doc/version20/Client95/

  OR

  download the .PDF file:

  http://www.backweb.com/doc/version20/bwuser.pdf

- 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.

E Additional Command-line Utilities

Using the Service Password utility

The Service Password utility (SVCPWD) is a command-line utility that allows administrators to set and/or change service account information, such as user-names and passwords, that the McAfee Services use to operate.

When SVCPWD.EXE runs, it looks for a plain text file that specifies what computers to modify the service accounts for.

To create this text file use any text editor, such as Notepad. List the computers that you want to update service account information for.

Example:

\\COMPUTER1

\\COMPUTER2

\\SERVER

To run the SVCPWD utility, follow these steps:

1. Set service accounts to user "LocalSystem". If a domain\username is entered, the SVCPWD utility will require a password for the domain\username.

   ✍ *The domain\username that is used by the services must be from an administrative account*

2. Enter SVCPWD and the name of the text file at a command prompt and push ENTER:

   Example:

   ```
   C:\SVCPWD yourfile.txt
   ```

   ✍ *Use* `SVCPWD/?` *for additional command-line options.*

3. Enter the new username and password and press ENTER.

   Response: The SVCPWD utility contacts the computers listed in the text file through the network, then changes the username and password given to McAfee Services.

Using the IMPTASK utility

IMPTASK is a command-line utility for broadcasting tasks to multiple servers. To use IMPTASK, use the following syntax at the command prompt:

Syntax

```
IMPTASK /FILE filename [/Server \\computer]
```

`filename` Specifies the configuration file to import.

`\\computer` Specifies the UNC name of the computer to receive the file.

Examples

```
IMPTASK /FILE mytask.vsc
```
Imports the file MyTask.vsc to the local computer.

```
IMPTASK /FILE YourTask.vsc /SERVER \\YourServer
```
Imports the file YourTask.vsc to the computer named YourServer.

F Reference

VirusScan Command-line Options

The following table lists all of the NetShield command options you can use when you're running ViruScan in DOS from the command-line.

Example of options:

SCAN32 [object1] [object2 . . .] [object1] [object2 . . .]

SCAN32 [<switches>] [<scanitem>]

SCAN32 <config.VSC> [<override_switches>] [<override_scanitem>]

SCAN32 [/SERVER <servername>] /TASK <taskid> [<override_switches>] [<override_scanitem>]

Command-line Option	Description
/[NO]SPLASH	Displays initial splash screen. Default: /SPLASH
/[NO]AUTOSCAN	VirusScan automatically initiates scanning when started. Default: <depends on UI type>
/[NO]AUTOEXIT	VirusScanVirusScan automatically exits if no viruses are found. If viruses are found, VirusScan does not exit (see /ALWAYSEXIT). Default: <depends on UI type>

Command-line Option	Description
/[NO]ALWAYSEXIT	VirusScan automatically exits when scan is complete. VirusScan exits even if viruses are detected (see /AUTOEXIT). Default: <depends on UI type>
/[NO]SUB	Scans all subfolders. Default: /SUB
/[NO]ALL	Scans all files, regardless of their file extension. Default: /NOALL
/[NO]COMP	Scans compressed files and ZIP files. Default: /COMP
/UICONFIG|/ UIEXONLY|/ UINONE	Specifies the type of graphical user interface displayed: UICONFIG - A fully-configurable interface that allows the user to specify which items to scan. UIEXONLY - An “execution-only” interface that takes all options from the command line, registry, or VSC file. This value implies /AUTOSCAN and /AUTOEXIT. UINONE - No visible user interface. All options must be taken from the command line, registry or VSC file. Activity logging should be used to obtain the scan results. This value implies /AUTOSCAN and /ALWAYSEXIT. Default: /UICONFIG

Command-line Option	Description
/CONTINUE|/PROMPT|/CLEAN|/DELETE|/MOVE <FOLDER>	Specifies what action to take when a virus is detected: CONTINUE - Logs information about the infection and continues scanning. PROMPT - Pauses the scan to ask the user which action to take (see /MSG). CLEAN - Attempts to clean the infected item and continues with the scan. DELETE - Attempts to delete the infected item and continues with the scan. MOVE - Attempts to move the infected files and continues scanning. Default: /CONTINUE
/[NO]MSG <message>	Displays a custom message when the /PROMPT option is specified and a virus is detected. Default: /NOMSG
/[NO]BEEP	Plays an audible tone on completion of a scan if infected items were found. Default: /BEEP
/RPTSIZE <n>	Specifies the maximum size of the activity log file (in kilobytes). When the file exceeds this size, it is truncated to zero bytes. Default: /RPTSIZE 100
/[NO]MEM	Performs a memory scan. Default: /MEM
/[NO]BOOT	Performs a boot record scan. The Master Boot Record (MBR) is scanned and the boot sector of each drive where a scan item resides is scanned. Default: /BOOT

Command-line Option	Description
`/EXT extensions`	Lists the file extension types to scan, unless the /ALL option is specified. To modify this list, the entire list must be entered with each entry separated by a space, for example: /EXT “EXE COM SYS ZIP”. Default: /EXT “EXE COM BIN SYS DO? OVL DLL APP CMD”
`/DEFEXT extensions`	A list of program extensions to default to when user selects “New Scan” from the configurable (see /CONFIG) user interface. The entire list must be quoted and each entry separated by a space, for example: /DEFEXT “EXE COM SYS ZIP”. Default: /DEFEXT “EXE COM BIN SYS DO? OVL DLL APP CMD PRG”
`/PRIORITY <n>`	Sets the priority of the scan process using a value between 1 and 5. Default: /PRIORITY 3
`/TASK <taskid>`	Specifies: (a) configuration data should be read from the registry. The taskid is a registry key found under: HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\NetShieldVirusScan\Tasks. This parameter may be used with or without the /SERVER option. If /SERVER is omitted, the local registry is used. (b) when used with the /CANCEL option, the task is terminated. Default: (none)
`/SERVER <servername>`	Specifies that configuration data should be read from the registry on the specified server. The /TASK option must be used with this parameter. Default: (none)

Command-line Option	Description
/CANCEL	Specifies that a running task should be canceled. The /TASK parameter must be used with this option to specify which task is to be canceled. Default: (none)
/[NO]LOG [<log-file>]	Enables activity logging and optionally, changes the name of the log file. Default: /LOG “NetShield VirusScan Activity Log.txt”
/LOGALL	Specifies that all scan activity is logged. This option is equivalent to specifying /LOGDETECT /LOG-CLEAN /LOGDELETE /LOGMOVE /LOGSET-TINGS /LOGSUMMARY /LOGDATETIME / LOGUSER Default: /LOGALL
/[NO]LOGDETECT	Logs the detection of infected items. Default: /LOGDETECT
/[NO]LOGCLEAN	Logs the results of attempts to clean infected items. Default: /LOGCLEAN
/[NO]LOGDELETE	Logs the results of attempts to delete infected items. Default: /LOGDELETE
/[NO]LOGMOVE	Logs the results of attempts to move infected items. Default: /LOGMOVE
/[NO]LOGSETINGS	Logs the list of configuration settings used for each scan. Default: /NOLOGSETTINGS
/[NO]LOGSUMMARY	Logs a summary of the completed scan. Default: /LOGSUMMARY

Command-line Option	Description
/[NO]LOGDAETIME	Timestamps each entry in the log file. Default: /LOGDATETIME
/[NO]LOGUSER	Stamps each entry in the log file with the name of the user who executed the scan. Default: /LOGUSER
Not Supported	Exclusions Multiple Scan Items
/? or /HELP	Does not scan. Instead, displays a list of VirusScan command-line options with a brief description of each. Use either of these options alone on the command line (with no other options).
/ADL	Scans all local drives (including compressed, CD-ROM, and PCMCIA drives, but not diskettes), in addition to those specified on the command line. To scan both local and network drives, use /ADL and /ADN together in the same command line.
/ADN	Scans all network drives for viruses, in addition to those specified on the command line. To scan both the local drives and network drives, use /ADL and /ADN together in the same command line.

Command-line Option	Description
`/AF filename`	Stores validation/recovery codes in *filename.* Helps you detect new or unknown viruses. /AF logs validation and recovery data for executable files, the boot sector, and master boot record on a hard disk or diskette in a file you specify. The log file is about 89 bytes per file validated. You must specify a *filename*, which can include the full path. If the target path is a network drive, you must have rights to create and delete files on that drive. If *filename* exists, VirusScan updates it. /AF adds about 300% more time to scanning. ✍ */AF performs the same function as /AV, but stores its data in a separate file rather than changing the executable files themselves.* *The /AF option does not store any information about the master boot record or boot sector of the drive being scanned.*
`/ALL`	Overrides the default settings by scanning more files. By default, VirusScan checks files with .COM, .EXE, .SYS, .BIN, .OVL, .DLL, .DOC, and .DOT extensions, which are the files most likely to be infected by a virus. This option substantially increases the scanning time required. Use it if you have found a virus or suspect one. ✍ *The list of extensions for standard executables has changed from previous releases of VirusScan.*
`/APPEND`	Used in conjunction with /REPORT, appends the report message text to the specified report file, if it exists. Otherwise, the /REPORT option overwrites the specified report file, if it exists.

Command-line Option	Description
/AV	To help you detect and recover from new or unknown viruses, /AV adds recovery and validation data to each standard executable file (.EXE, .COM, .SYS, .BIN, .OVL, and .DLL), increasing the size of each file by 98 bytes. To update files on a shared network drive, you must have update access rights. To exclude self-modifying or self-checking files, and damaged files that might cause false alarms, use the /EXCLUDE option. Using any of the /AV, /CV, or /RV options together in the same command line returns an error. ✍ *The /AV option does not store any information about the master boot record or boot sector of the drive being scanned.*
/BOOT	Scans only the boot sector and master boot record on the specified drive.
/CF filename	Helps you detect new or unknown viruses. Checks validation data stored by the /AF option in *filename*. If a file or system area has changed, VirusScan reports that a viral infection may have occurred. The /CF option adds about 250% more time to scanning. Using any of the /AF, /CF, or /RF options together in a command line returns an error. ✍ *Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. If you use /CF, VirusScan continuously reports that the boot sector has been modified even though no virus may be present. Check your computer's reference manual to determine whether your PC has self-modifying boot code.*

Command-line Option	Description
`/CONTACTFILE filename`	Identifies a file containing a message string to display when a virus is found. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation. Any character is valid except a backslash (“\”). Messages that begin with a slash (“/”)or a hyphen (“-”) should be placed in quotation marks.
`/CV`	Helps you detect new or unknown viruses. Checks validation data added by the /AV option. If a file is modified, VirusScan reports that a viral infection may have occurred. The /CV option adds about 50% more time to scanning. Using any of the /AV, /CV, or /RV options together in the same command line returns an error. ✍ *The /CV option does not check the boot sector for changes.*
`/EXCLUDE filename`	Excludes any files listed in *filename* from the scan. This option allows you to exclude files from /AF and /AV validation and /CF and /CV checking. Self-modifying or self-checking files can cause a false alarm during a scan.
`/FAST`	Speeds up the scan. Reduces scanning time by about 15%. Using the /FAST option, VirusScan examines a smaller portion of each file for viruses. Using /FAST might miss some infections found in a more comprehensive (but slower) scan. Do not use this option if you have found a virus or suspect one.

Command-line Option	Description
`/FREQUENCY hours`	The number of hours that must occur between subsequent successful scans. In environments where the risk of viral infection is very low, use this option to prevent unnecessary or too-frequent scans. The lower the number of *hours* specified, the greater the scan frequency and the greater your protection against infection.
`/LOAD filename`	Uses the VirusScan settings stored in *filename.* VirusScan gets its settings from the default configuration file, DEFAULT.CFG, which is delivered with BootShield. You can specify any additional options on the command line. Alternatively, you can store all custom settings in a separate configuration file (an ASCII text file), then use /LOAD to load those settings from that file. Use the /LOAD *filename* command-line option to perform a scan using the information saved in this file. For example, if you have created a configuration file called FLOPPY.CFG, enter: `scan /load floppy.cfg` The above command line initiates a scan using its internal default settings plus any options specified in FLOPPY.CFG.
`/LOCK`	Halts the system to stop further infection if VirusScan finds a virus. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. If you use /LOCK, we recommend you use it with /CONTACTFILE to tell users what to do or whom to contact if a virus is found and the system locks up.
`/LOG`	Stores the time and date VirusScan is being run by updating or creating a file called SCAN.LOG in the root of the current drive.

Command-line Option	Description
`/MACROHEUR x` `(where x equals 0, 1, 2, 3, 4, 5, or 100)`	Adjusts the level of sensitivity used when performing heuristic scanning for possible macro viruses in Microsoft Word documents. 0 - turns off the heuristic scanning option for macro viruses. 1 (minimum) through 5 (maximum) - turns on heuristic scanning at varying levels of sensitivity. 100 - causes VirusScan to detect all macros, including those not found to be viral or probably viral. If 100 is chosen, VirusScan reports "This file contains macros" each time it detects a Microsoft Word file that contains a macro. The default setting is 5 (maximum).
`/MANY`	Scans multiple diskettes consecutively in a single drive. VirusScan prompts you for each diskette. Once you have established a virus-free system, use this option to check multiple diskettes quickly. The VirusScan program should reside on a disk that will not be removed during the scan. For example, if you are scanning disks in the computer's A: drive, and you are running the program from a disk in the A: drive, the program will become unavailable as soon as you remove the diskette to put another in. The following command causes an error during execution: `a:\scan a: /many`
`/MEMEXCL`	Exclude memory area from scanning. (The default is A000-FFFF, 0000=Scan all.) This command-line option has been added to prevent VirusScan from checking areas in upper memory which might contain memory-mapped hardware and might cause false alarms.

Command-line Option	Description
/MOVE directory	Moves all infected files found during a scan to the specified directory. To preserve drive and directory structure, this option has no effect if the Master Boot Record or Boot Sector is infected, since these are not actually files.
/NOBEEP	Disables the tone that sounds whenever VirusScan finds a virus.
/NOBREAK	Disables CTRL-C and CTRL-BREAK during scans. Users will not be able to halt scans in progress using CTRL-C or CTRL-BREAK. Use this option in conjunction with /LOG to create a meaningful audit trail of regularly scheduled scans.
/NOCOMP	Skips checking of compressed executables created with the LZEXE or PKLITE file compression programs. Reduces scanning time when a full scan is not needed. Otherwise, by default, VirusScan checks inside executable, or self-decompressing, files that have been created using the LZEXE or PKLITE file compression programs. VirusScan decompresses each file in memory and checks for virus signatures, which takes time but results in a more thorough scan. If you use /NOCOMP, VirusScan does not check inside compressed files for viruses, although it can check for modifications to those files if they have been validated using validation/recovery codes. ✍ *VirusScan does not check compressed files, such as .ZIP and .ARC files.*
/NODDA	No direct disk access. Prevents VirusScan from accessing the boot record. This feature has been added to allow VirusScan to run under Windows NT. You might need to use this option on some device-driven drives.

Command-line Option	Description
/NOEMS	Prevents VirusScan from using expanded memory (LIM EMS 3.2), ensuring that EMS is available to other programs.
/NOEXPIRE	Disables the “expiration date” message if the VirusScan data files are out of date.
/NOMEM	Reduces scan time by omitting all memory checks for viruses. Use /NOMEM only when you are absolutely certain that your computer is virus-free. VirusScan can check system memory for all critical known computer viruses that can inhabit memory. In addition to main memory from 0Kb to 640Kb, VirusScan checks system memory from 640Kb to 1088Kb that can be used by computer viruses on 286 and later systems. Memory above 1088Kb is not addressed directly by the processor and is not presently susceptible to viruses.
/PAUSE	Enables screen pause. If you specify /PAUSE, the “Press any key to continue” prompt appears when VirusScan fills up a screen with messages (for example, when you’re using the /SHOWLOG or /VIRLIST options). Otherwise, by default, VirusScan fills and scrolls a screen continuously without stopping, which allows VirusScan to run on PCs with many drives or that have severe infections without requiring you to attend. We recommend that you omit /PAUSE when keeping a record of VirusScan’s messages using the report options (/REPORT, /RPTCOR, /RPTMOD, and /RPTERR).

Command-line Option	Description
/PLAD	Preserve last access dates (on proprietary drives only). Prevents changing the last access date attribute for files stored on a network drive in a proprietary network. Normally, proprietary network drives update the last access date when VirusScan opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use /PLAD to ensure that the last access date does not change as the result of scanning.
/REPORT *file-name*	Creates a report of infected files and system errors. Saves the output of VirusScan to *filename* in ASCII text file format. If *filename* exists, /REPORT erases and replaces it (or, if you use /APPEND, adds the report information to the end of the existing file). You can include the destination drive and directory (such as D:\VSREPRT\ALL.TXT), but if the destination is a network drive, you must have rights to create and delete files on that drive. You can also use /RPTALL, /RPTCOR, /RPTMOD, and /RPTERR to add scanned files, corrupted files, modified files, and system errors to the report.
/RF *filename*	Removes recovery and validation data from *filename* created by the /AF option. If *filename* resides on a shared network drive, you must be able to delete files on that drive. Using any of the /AF, /CF, or /RF options together in the same command line returns an error.
/RPTALL	Adds list of files scanned to the report file (used with /REPORT).

Command-line Option	Description
/RPTCOR	When used in conjunction with /REPORT, adds the names of corrupted files to the report file. A corrupted file may be a file that has been damaged by a virus. You can use /RPTCOR with /RPTMOD and /RPTERR on the same command line. ✍ *There may be false readings in some files that require an overlay or another executable to run properly (that is, a file that is not executable on its own).*
/RPTERR	Adds a list of system errors to the report file. This option is used in conjunction with /REPORT. System errors include problems reading or writing to a diskette or hard disk, file system or network problems, problems creating reports, and other system-related problems. You can use /RPTERR with /RPTCOR and /RPTMOD on the same command line.
/RPTMOD	Adds list of modified files to the report file. This option is used in conjunction with /REPORT. VirusScan identifies modified files when the validation/recovery codes do not match (using the /CF or /CV options). You can use /RPTMOD with /RPTCOR and /RPTERR on the same command line.
/RV	Removes validation and recovery data from files validated with the /AV option. To update files on a shared network drive, you must have access rights to update them. Using any of the /AV, /CV, or /RV options together in the same command line returns an error.

Command-line Option	Description
/SHOWLOG	Displays the contents of SCAN.LOG. SCAN.LOG stores the time and date VirusScan is being run by updating or creating a file called SCAN.LOG in the current directory and the date and time of previous scans that have been recorded in the SCAN.LOG file using the /LOG switch. The SCAN.LOG file contains text and some special formatting. To pause when the screen fills with messages, specify the /PAUSE option.
/SUB	Scans subdirectories inside a directory. By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories inside any directories you have specified. Do not use /SUB if you are scanning an entire drive.
/VIRLIST	Displays the name and a brief description of each virus that VirusScan detects. To pause when the screen fills with messages, specify the /PAUSE option. Use /VIRLIST alone or with /PAUSE on the command line. You can save the list of virus names and descriptions to a file by redirecting the output of the command. For example, in DOS, enter: `scan /virlist > filename.txt` ✍ *Because VirusScan can detect many viruses, this file is more than 50 pages long.*

Scan command option examples

The following examples show the VirusScan command using various option settings. Remember that you can use the DEFAULT.CFG file to specify the commands used each time VirusScan is run.

✍ *These examples show how to scan all files, not just the boot sector.*

- To scan your computer's C: drive:

  ```
  scan c:

  VirusScan checks executable files on C:, plus the boot
  sector and boot master record and RAM memory file
  viruses.
  ```

- To scan the computer's boot sector and master boot record:

  ```
  scan c: /boot

  This command also scans memory.
  ```

- To scan executable files on drive F:, a network drive:

  ```
  scan f:
  ```

- To scan executable files on multiple diskettes on drive A:

  ```
  scan a: /many

  VirusScan checks the diskette in drive A:, then prompts
  the user to insert more disks to continue checking.
  This command also scans the diskette's boot sectors.
  ```

- To scan all local and network drives (including compressed, CD-ROM, and PCMCIA drives, but not diskettes):

  ```
  scan c: /adl /adn
  ```

- To scan for viruses in files and add validation codes to executable files on drives C:, D:, and E:

  ```
  scan c: d: e: /av /all
  ```

- To scan for viruses on network drive M: and create a log file of infections, corruptions, and errors in the file INFECTN.RPT on drive D:

  ```
  scan m: /report d:\infectn.rpt /rptcor /rpterr /append
  ```

  ```
  If D:\INFECTN.RPT .ALReady exists, VirusScan appends
  the new information to the existing report file.
  ```

- To scan files in the directories USER\MAC, USER\BILL, and USER\DAVE:, including their associated subdirectories, on drive E:

  ```
  scan e:\user\mac e:\user\bill e:\user\dave /sub /all
  ```

- To quickly scan drives C:, D:, and E: and report any executable files that have associated validation codes and have been modified:

  ```
  scan c: d: e: /fast /cv
  ```

- To scan a single file, in this case COMMAND.COM:

  ```
  scan c:\command.com
  ```

VSC File Format

The VSC file is a configuration text file, formatted similarly to the Windows INI file, which outlines VirusScan'sNetShield's settings. Each variable in the file has a name followed by the equal (=) sign and a value. The values define which settings were selected for the configuration.

The variables are arranged in five groups: ScanOptions, AlertOptions, Activity-LogOptions, Scheduler, and TaskDefinitions. To edit the VSC file, right-click the filename and select Edit.

ScanOptions

Variable	Description
szProgramExten-sions	Type: String Defines extensions to be used as program exten-sions during scan Default value: EXE COM DLL SYS DO?
szDefaultPro-gramExtensions -	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: EXE COM DLL SYS DO?
bIncludeSubFolders	Type: Boolean (1/0) Instructs scanner to search for viruses inside sub-folders Default value: 1
bScanAllFiles	Type: Boolean (1/0) Instructs program to scan inside all files Default value: 0

Variable	Description
bScanCompressed	Type: Boolean (1/0) Instructs program to scan inside compressed files (PkLite, LZEXE, ZIP) Default value: 1
uScanAction	Type: Integer (1-5) Defines what action will be taken upon virus detection: 1 - Prompt for Action 2 - Continue Scanning 3 - Move Infected File 4 - Clean Infected File 5 - Delete Infected File Default value: 1
bAutoStart	Type: Boolean (1/0) Defines if scan will be started immediately upon launch Default value: 0
bAutoExit	Type: Boolean (1/0) Defines if scanner will be unloaded when scan is finished Default value: 0
nPriority=0	Type: Integer (0-5) Defines the priority at which scan is to be executed Default value: 3
szScanItem=C:\	Type: String Defines item to be scanned Default value: C:\

AlertOptions

Variable	Description
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed upon virus detection Default value: 1
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection Default value: Your custom message here!
bSoundAlert	Type: Boolean (1/0) Defines if audible alert should be made upon virus detection Default value: 1

ActivityLogOptions

Variable	Description
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 1
bLimitSize	Type: Boolean (1/0) Defines if size of the log file should be limited Default value: 1
uMaxKilobytes	Type: Integer Defines maximum size of the log file Default value: 100
szLogFileName	Type: String Defines log file name Default value: NetShield VirusScan Activity Log.txt
bLogDetection	Type: Boolean (1/0) Defines if scan results should be logged Default value: 1
bLogClean	Type: Boolean (1/0) Defines if clean results should be logged Default value: 1
bLogDelete	Type: Boolean (1/0) Defines if infected file delete operations should be logged Default value: 1
bLogMove	Type: Boolean (1/0) Defines if infected file move operations should be logged Default value: 1

Variable	Description
bLogSettings	Type: Boolean (1/0) Defines if session settings should be logged Default value: 1
bLogSummary	Type: Boolean (1/0) Defines if session summary should be logged Default value: 1
bLogDateTime	Type: Boolean (1/0) Defines if time and date of an event should be logged Default value: 1
bLogUserName	Type: Boolean (1/0) Defines if user name should be logged Default value: 1

TaskDefinition

Variable	Description
szTaskName	Type: String Defines task name Default value: New Scan Task
wTaskAttrib	Type: Integer Contains task attributes Do not modify
wTaskType	Type: Integer Contains task type Do not modify

Scheduler

Variable	Description
bSchedEnabled	Type: Boolean (1/0) Enables scheduling for the task Default value: 0
wFlags	Type: Integer Contains task flags Do not modify
wTime	Type: Integer Defines time when task is to be launched Do not modify
wDate	Type: Integer Defines date when task is to be launched Do not modify

Centralized Alerting .ALR File Format

The .ALR file is a text file that contains Centralized Alerting virus event variables. Each variable in the file has a name followed by the equal (=) sign and a value. The following is a line-by-line description of the Centralized Alerting .ALR file format:

Variable	Description
[CentralAlert]	Centralized Alerting identifier
uFileVersion	Type: Integer Centralized Alerting version number
uStatus	Reserved
szVirusName	Type: String The name of the virus.
szItemName	Type: String The infected file name and path.
szUserName	Type: String The user name.
szSoftware	Type: String The name of the Network Associates virus application installed on the reporting machine.
szSoftwareVersion	Type: String The version of the virus application.
szComputerName	Type: String The name of the machine reporting the event.
uYear	Type: Integer (0000-9999) The year of the event.
uMonth	Type: Integer (1-12) The month of the event.
uDay	Type: Integer (1-31) The day of the event.
uHour	Type: Integer (0-23) The hour of the event .

uMinute	Type: Integer (0-59) The minute of the event.
uSecond	Type: Integer (0-59) The second of the event.

Index

A

advanced options 108
Alert Manager 69
  audible alerting 94
  DMI alerting 90
  E-mail notification 78
  Forward page 72
  logging alerts 96
  Network message page 75
  Pager notification 81
  Print notification 85
  SMTP 78
  SNMP notification 88
  summary page 71
Alert options 68
Alerts
  changing priorities 101
  customizing 100
  enabling/disabling 100
  executing a program 88
  message variables 102
  program launch 92
audible alerts 94
Automatic DAT Update task 105
Automatic Product Upgrade 109
AutoUpdate 104, 108
  Automatic Product Upgrade 109
  scheduling 114
AutoUpgrade
  advanced options 112

B

Boot record
  preventing VirusScan from accessing 170
Boot sector
  limiting scan to 166
BootShield components
  VirusScan 175–176
broadcasting network messages 75
Bulletin Board System (BBS) 16

C

command-line options 156, 159
Compressed files
  skipping during virus scans 170
Compressed Files checkbox 43, 56
Console
  last results display area 33
  the status bar 33
  the task display area 33
Control Break
  disabling during scans 170
Control C
  disabling during scans 170
Copying and pasting tasks 38
Customer Care
  contacting 16

D

Data files
  additional 134
  common 134
Dates
  preventing VirusScan from changing 172
Default settings
  creating multiple configuration files 168
DEFAULT.CFG
  using a different configuration file 168
Deleting tasks 39

Direct drive access
disabling with VirusScan 170
Directories
scanning 174
Disabling tasks 39
Diskettes
scanning multiple 169
Displaying list of detected viruses
with VirusScan 174
DMI alerting 90
Drives
scanning local 164
scanning network 164

E

EMS
preventing VirusScan from using 171
Excluding files
during virus scans 167
Expanded memory
preventing VirusScan from using 171
Expiration date message
disabling 171
Exporting tasks 36

F

Features
administrative 14
detection 14
protection 14
File types
determining which are scanned 165
Files
moving infected files 170
preventing VirusScan from changing last access dates 172
Floppy diskettes
scanning multiple 169
Frequency
determining for VirusScan 168

H

Help
displaying for Scan 164
Hunter 13

I

Importing tasks 37
IMPTASK utility 158
Infected files
moving 170
Installation 21
local 24
remote 26
silent 28
Introduction 12

L

Last access date
preventing VirusScan from changing 172
Local drives
scanning 164
Locking the system
if a virus is found 168
Log file
creating with VirusScan 168
displaying 174
logging 61
alerts 96
LZEXE
and VirusScan 170

M

Main features 14
Memory
excluding area from scans 169
omitting from scans 171
preventing VirusScan from using expanded 171
Messages
displaying when a virus is found 167
pausing when displaying 171
Moving
infected files 170

N

NetShield
Installing 21
Introduction 12
what is 13
NetWare drives
and VirusScan 172
Network Associates
consulting 129
contacting
BBS 16

Customer Care 16
outside the United States 18
via America Online 17
via CompuServe 16
within the United States 17
customer service programs 126
Enterprise support 130
Jump Start program 130
professional services programs 129
support services 125
training 17, 129
Network drives
scanning 164
Notification 68
Novell NetWare 34

O

On-access task 40
choosing files 42
editing 41
excluding folders 50
logging activity 48
on-demand scans 61
On-demand tasks 53
creating 53
editing 54
excluding folders 65
logging 61
NetShield response 58
scheduling 63
using Scan32 121
Options
see Scan command-line options

P

password utility 156
Pausing
when displaying VirusScan messages 171
PKLITE
and VirusScan 170
PKZIP
and VirusScan 170
program file extensions
default 44, 56, 121
Program launch on alert 88, 92

R

Recovery codes
using with VirusScan 165
Recovery data
adding to executable files 166
removing 172, 173
Remote 34
remote administration 34
reporting viruses not detected 19
Reports
adding names of corrupted files to 173
adding names of modified files to 173
adding names of scanned files to 172
adding system errors to 173
generating with VirusScan 165, 172
responding to virus infections 45

S

Scan
reporting options 123
using 121
what is? 120
SCAN.LOG
creating a log 168
displaying 174
Scanning
on-access 40
on-demand 53
scanning
Hunter 13
scheduling
updates/upgrades 114
SecureCast
additional files delivered by 134
common data files delivered by 134
Enterprise SecureCast 133, 150
benefits 150
completing registration for 150
setting up 151

troubleshooting 153
unsubscribing 154
using 152
features 135
free services 135
Home SecureCast 133, 136
completing registration for 137
downloading automatically 136
registering evaluation software 146
setting up 136
unsubscribing 137
updating registered software 138
using 137
initiating a download 138
support resources 155
system requirements 135
updating your software with 133
Service Password utility 156
Silent installation 28
SNMP 88
Statistics window 36
Subdirectories
scanning 174

T

Tasks
copying and pasting 38
deleting 39
disabling 39
exporting 36
importing 37
on-demand 53
tasks
Automatic DAT Update 105
Automatic Product Upgrade 109
on-access scan 40
technical support
e-mail address 16
information needed from user 17
Network Associates Bulletin Board System (BBS) 16
online 16
Training
scheduling 17
training for Network Associates products 17

U

Updating
AutoUpdate 104
DAT files 105
overview 103
product upgrade 109
SecureCast 133
sheduling updates 114
Upgrading NetShield 110

V

Validate 116
Validating NetShield 116
Validation codes
using with VirusScan 165
Validation data
adding to executable files 166
checking 167
checking during virus scans 166
removing 172, 173
VIRNOTFY.EXE 93
Virus notification 68
Virus scanning
excluding files 167
excluding the memory area 169
file types scanned 165
including subdirectories 174
local drives 164
macro viruses 169
moving infected files 170
multiple diskettes 169
network drives 164
preventing users from halting 170
skipping compressed files 170
speeding up 167
system memory 171

Viruses
displaying a list of detected 174
locking the system if found 168
what are ix
viruses
encountering 117
removing 117
reporting new viruses 19
VirusScan
and expanded memory 171
command examples 175
disabling the expiration date message 171
displaying a message when a virus is found 167
displaying list of detected viruses 174
excluding files 167
excluding memory area from scans 169
generating a report file 165, 172, 173
locking the system 168
multiple diskettes 169
preventing users from halting 170
scanning only the boot sector 166
setting the scan frequency 168
speeding the scan 167
validation 167, 172
VirusScan command-line options
/? or /HELP 164
/ADL 164
/ADN 164
/AF 165
/ALL 165
/APPEND 165
/AV 166
/BOOT 166
/CF 166
/CONTACTFILE 167
/EXCLUDE 167
/FAST 167
/FREQUENCY 168
/LOAD 168
/LOCK 168
/LOG 168
/MACROHEUR 169
/MANY 169
/MEMEXCL 169
/MOVE 170
/NOBEEP 170
/NOBREAK 170
/NOCOMP 170
/NODDA 170
/NOEMS 171
/NOEXPIRE 171
/NOMEM 171
/PAUSE 171
/PLAD 172
/REPORT 172
/RPTALL 172
/RPTCOR 173
/RPTERR 173
/RPTMOD 173
/RRF 172
/RV 173
/SHOWLOG 174
/SUB 174
/VCV 167
/VIRLIST 174
VSC file format 177

W

Windows 95
using VirusScan with 170
Windows for Workgroups
using VirusScan with 170