User’s Guide

NetShield for Windows NT

McAfee, Inc.
2710 Walsh Avenue
Santa Clara, CA 95051-0963

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

FAX: (408) 970-9727
BBS: (408) 988-4004

COPYRIGHT

TRADEMARK NOTICES

McAfee, McAfee Associates, VirusScan, NetShield, and Site Meter are registered trademarks of McAfee Associates, Inc. WebScan, SiteExpress, BootShield, ServerStor, ScreenScan, PCCrypto, WebCrypto, eMail-It, GroupScan, GroupShield, NetCrypto, Remote Desktop 32, WebShield, and NetRemote are trademarks of McAfee Associates, Inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

“SABRE” is a trademark of American Airlines, Inc. and is licensed for use to McAfee. Saber Software is not affiliated with American Airlines, Inc. or SABRE Travel Information Network. All trademarks are the property of their respective owners.

FEEDBACK

McAfee 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: McAfee, Inc., Documentation, 2710 Walsh Avenue, Santa Clara, CA 95051-0963, or send a fax to McAfee Documentation at (408) 653-3143.

Issued October 1996/NetShield NT v2.5.2

Table of Contents

1

Introducing NetShield

What is NetShield for Windows NT?

NetShield for Windows NT is a client-server application with the NetShield Server software comprising the server end of the relationship and the NetShield Console comprising the client end of the relationship. 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.

Most of the functionality of NetShield for Windows NT is built into the Console.

Main Features

Superior detection

Consistently detects over 96% of the more than 8,500 known viruses.

NCSA certified—McAfee participates in establishing virus identification standards with the National Computer Security Association.

Uses patented Code Trace, Code Poly, and Code Matrix technology to accurately pinpoint known generic and unknown boot, file, multi-partite, stealth, mutating, polymorphic, encrypted, and macro viruses.

Automated protection

Supports Windows NT services and file system.

Real-time scanning of all file accesses with minimal resource utilization.

Flexible scheduling and immediate scanning options.

Advanced alerting features including alphanumeric pager, e-mail via SMTP, and NT event logging.

Administrative ease

Scan Wizard assists users in creating new scan tasks.

AutoUpdate feature allows for immediate or scheduled updating via a central shared location or FTP download.

Enhanced virus encyclopedia enables users to learn more about various virus types.

How To Contact Us

Customer service

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

McAfee, Inc.
2710 Walsh Avenue
Santa Clara, CA 95051-0963
U.S.A.

Technical support

McAfee is famous for its dedication to customer satisfaction. McAfee has continued this tradition by investing considerable time and effort to make our website a valuable resource for updating McAfee software and obtaining the latest news and information. For technical support information and issues, we encourage you to visit our website first.

World Wide Web	http://www.mcafee.com

If you do not find what you need or do not have access to the Web, try one of McAfee's automated services.

Automated Voice and Fax Response System	(408) 988-3034
Internet	support@mcafee.com
McAfee 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

Microsoft Network (MSN)	MCAFEE

If the automated services did not solve your problem, you may contact McAfee Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

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

To speed the process of helping you use our products, please note the following before you call:

- Product name and version
- Computer brand, model, and any additional hardware
- Operating system type and version
- Service Packs installed
- Network protocols used
- Services and devices loaded
- Specific steps to reproduce the problem, if applicable

McAfee training

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

International contact information

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

McAfee Canada
178 Main Street
Unionville, Ontario
Canada L3R 2G9
Phone: (905) 479-4189
Fax: (905) 479-4540

McAfee Europe B.V.
Orlyplein 81 - Busitel 1
1043 DS Amsterdam
The Netherlands
Phone: (0) 31 20 6815500
Fax: (0) 31 20 6810229

McAfee France S.A.
50 rue de Londres
75008 Paris
France
Phone: 33 1 44 908733
Fax: 33 1 45 227554

McAfee Deutschland GmbH
Industriestrasse 1
D-82110 Germering
Germany
Phone: 49 89 8943560
Fax: 49 89 89435699

McAfee (UK) Ltd.
Hayley House, London Road
Bracknell, Berkshire
RG12 2TH United Kingdom
Phone: 44 1344 304730
Fax: 44 1344 306902

2

Installing NetShield

Before You Start

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

Installation requirements

- Windows NT Server version 3.51 or later or Windows NT Workstation version 3.51 or later (for remote console administration of servers only)
- At least 1.5MB of free disk space to install the program files
- Latest version of Microsoft Service Pack

✍ *NetShield is an 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.*

Performing the Installation

To install NetShield NT, complete the following procedure:

✍ *NetShield NT 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.*

Step **Action**

1. Start the installation.

- Log on to the Windows NT server. You must have administrator security access to the Windows NT domain.

2. Do one of the following:

- If installing from the CD or diskettes, insert the CD or the first diskette.
- If installing from files downloaded from the BBS, 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 or diskettes, enter the following:

  ```
  x:\SETUP
  ```

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

- If installing from files you downloaded from the McAfee Web Site, enter the following:

  ```
  x:\path\SETUP
  ```

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

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

4. Click OK to begin the installation.

   Response: The NetShield NT Welcome Screen is displayed.

5. Click Next.

   Response: The Setup Type screen is displayed.

6. Select the destination directory for the NetShield NT program files.

7. Select the type of installation:

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

8. From the Service Account Information Screen, enter a user name with Administrator rights and a password. If this is a Backup Domain Controller, select the Backup Domain Controller checkbox. Click Next.

   ✍ *Do not use a password that will expire. If you select Skip, the service will be installed with the system account.*

   Response: The Confirm Installation Settings screen is displayed.

9. Confirm the installation options are correct and click Next.

   Response: NetShield NT is installed.

Once installed, it is strongly recommended you read the NetShield NT README.1ST and WHATSNEW.TXT files. These files contain important last-minute and licensing information.

3

Getting Started

Using the NetShield Console

Starting the Console

From the Program Manager, open the McAfee NetShield group and double-click the NetShield Console icon.

The Console is displayed and contains these components:

- the menu bar
- the toolbar
- the task display area
- the status bar

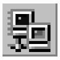
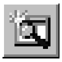
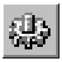
The menu bar

The menu bar contains the following menus and menu commands:

Scan	Edit	View	Tools	Help
New Task	Copy	Toolbar	Virus List	Help Topics
Scan Wizard	Paste	Status bar	AutoUpdate	About
Enable/ Disable/Start	Export	Refresh	Alerts	
Rename	Import	Options	Event Viewer	
Delete			Select Computer	
Statistics			Disconnect Computer	
Activity log				
Properties				
Exit				

The toolbar

The toolbar contains the following buttons:

Tool	Description (Corresponding Menu/Command)
	Connect to a server (Tools/Select Computer).
	Disconnect from a server (Tools/Disconnect Computer).
	Start the Scan Wizard (Scan/Scan Wizard).
	Create a new task (Scan/New Task).
	Edit a task’s properties (Scan/Properties).
	Copy a task (Edit/Copy).

Tool	Description (Corresponding Menu/Command)
📋	Paste a task (Edit/Paste).
✕	Remove a task from the Console (Edit/Delete).
▷	Start a scheduled task (Scan/Start and Scan/Enable).
■	Stop a scheduled task (Scan/Stop and Scan/Disable).
📋	View the virus list (Tools/Virus List).
📓	Open the NetShield Event Viewer (Tools/Event Log).

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 29.

To edit the on-access task, see "Editing the on-access task" on page 20.

✍ *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.

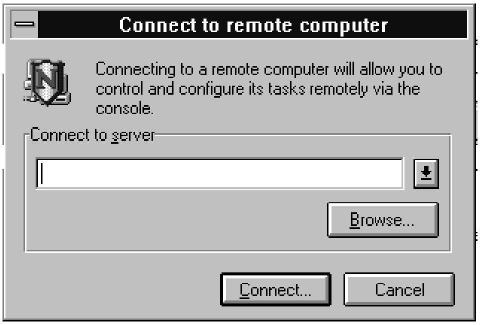
Changing Computers

When the NetShield 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 change computers, complete the following procedure:

Step **Action**

1. Click or select Select Computer from the Tools menu.

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



Connect to remote computer

Connecting to a remote computer will allow you to control and configure its tasks remotely via the console.

Connect to server

Figure 3-1. Connect to Remote Computer Dialog Box

2. Enter the UNC name of a server or click Browse to locate a server.

✍ *The target server must have the NetShield Server software installed.*

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 NetShield Console

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

What is a Task?

A task scans for viruses according to how it is configured. There are two types of tasks: on-access tasks and on-demand tasks.

The on-access task monitors files copied to and 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 20.

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 29.

The On-access Task

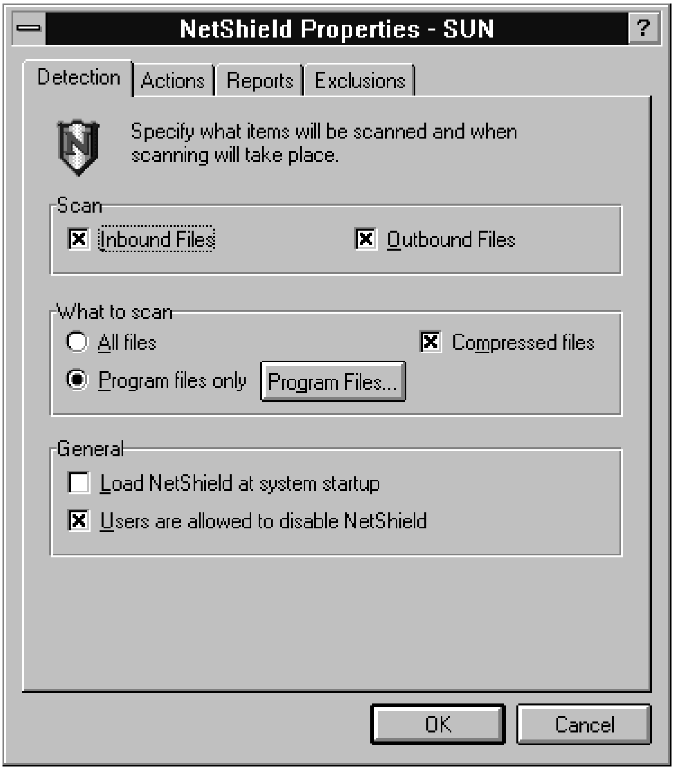
Editing the on-access task

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

To edit the name of the on-access task, highlight the text with your mouse and type a new name over “NetShield On-Access Task”.

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 sheet appears with the Detection page displayed.



Specify what items will be scanned and when scanning will take place.

Scan
☒ Inbound Files
☒ Outbound Files

What to scan
○ All files
● Program files only
☒ Compressed files

General
☐ Load NetShield at system startup
☒ Users are allowed to disable NetShield

Figure 4-1. NetShield Properties Sheet (Detection Page)

Choosing which files are scanned

To choose which files are scanned, complete the following procedure:

Step	Action
1.	Click the Detection tab of the NetShield properties sheet. **Response**: The Detection page appears (Figure 4-1).

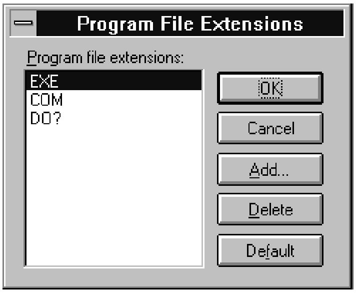
2. Select which files to scan:

   - To scan all inbound files, select the Inbound Files checkbox.
   - To scan all outbound files, select the Outbound Files checkbox.

3. Select the types of files to scan:

   - To scan all files, click the All Files option button. Skip to the next step.
   - To scan files with specific extensions, click the Program Files Only option button. Then click the Program Files button.

     Response: The Program File Extensions dialog box appears (Figure 4-2).



Program file extensions:
EXE
COM
DO?

Figure 4-2. Program File Extensions Dialog Box

   - ☐ 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. To include compressed files, select the Compressed Files checkbox.

5. To automatically start NetShield each time the server is started, select the Load NetShield at System Startup checkbox.

✍ *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.*

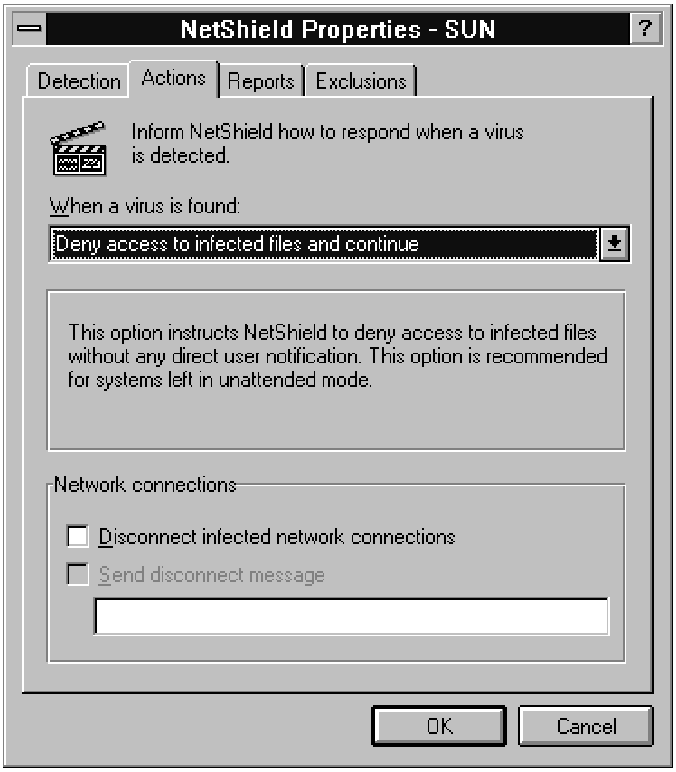
6. To allow disabling of the on-access task from the Console, select the Users Are Allowed To Disable NetShield checkbox.

7. 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.

Setting how NetShield responds to a virus infection

To control how NetShield responds to a virus detection, complete the following procedure:

Step	Action
1.	Click the Actions tab of the NetShield properties sheet. **Response**: The Actions page appears (Figure 4-3).



Inform NetShield how to respond when a virus is detected.

When a virus is found: Deny access to infected files and continue

This option instructs NetShield to deny access to infected files without any direct user notification. This option is recommended for systems left in unattended mode.

Network connections

☐ Disconnect infected network connections

☐ Send disconnect message

Figure 4-3. NetShield Properties Sheet (Actions Page)

2. Select how NetShield will respond to any viruses encountered. NetShield can respond by:

- Cleaning the infected files
- Deleting the infected files
- Denying access to the infected files
- Moving the infected files to a folder

3. Select whether NetShield will 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.*

   - To configure NetShield to disconnect infected network connections, select the Disconnect Infected Network Connections checkbox.

     ✍ *If a user is disconnected, run the appropriate McAfee anti-virus product to clean the system. Once the system is cleaned, use the Windows NT User Manager to reinstate access and synchronize the domain. For more information, refer to the documentation that accompanied Windows NT.*

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

4. 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.

Creating a virus activity log

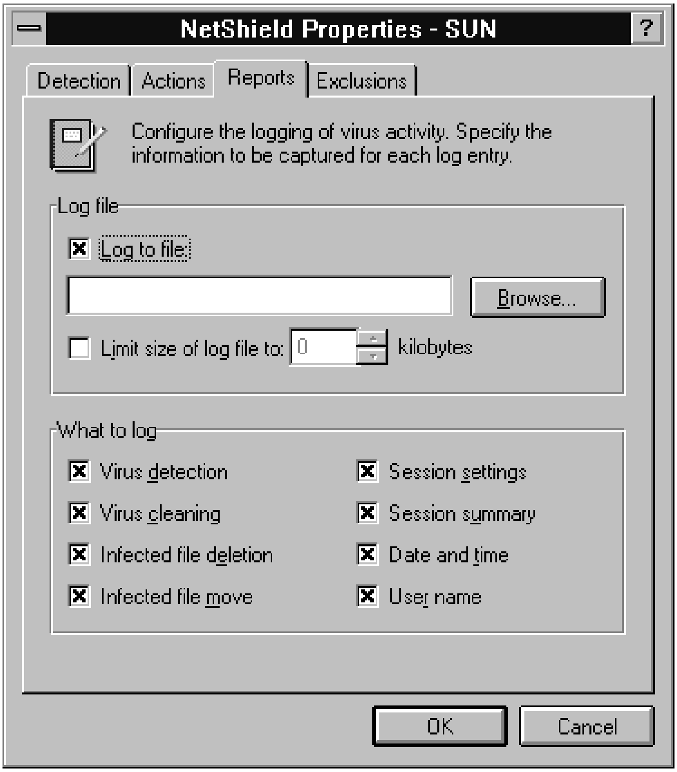
The virus information log keeps track of all relevant NetShield activity, including virus detection, virus cleaning, infected file deletion, infected file move, and session settings.

To configure the log file, complete the following procedure:

Step **Action**

1. Click the Reports tab of the NetShield properties sheet.

   Response: The Reports dialog page appears (Figure 4-4).



Configure the logging of virus activity. Specify the information to be captured for each log entry.

Log file

☒ Log to file:

☐ Limit size of log file to: 0 kilobytes

What to log

☒ Virus detection
☒ Virus cleaning
☒ Infected file deletion
☒ Infected file move
☒ Session settings
☒ Session summary
☒ Date and time
☒ User name

Figure 4-4. NetShield Properties Sheet (Reports Page)

2. Select the Log To File checkbox. To choose a new log file location, click Browse and select a location.

3. To limit the size of the log file, select the Limit Size checkbox and enter the maximum file size (in kilobytes).

4. Choose the type of activity to include in the log file. To include a type of activity, select the activity's checkbox.

5. 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 be configured to exclude specified files or folders from scanning.

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

To exclude folders from being scanned, complete the following procedure:

Step	Action
1.	Click the Exclusions tab of the NetShield properties sheet. **Response**: The Exclusions dialog page appears (Figure 4-5).

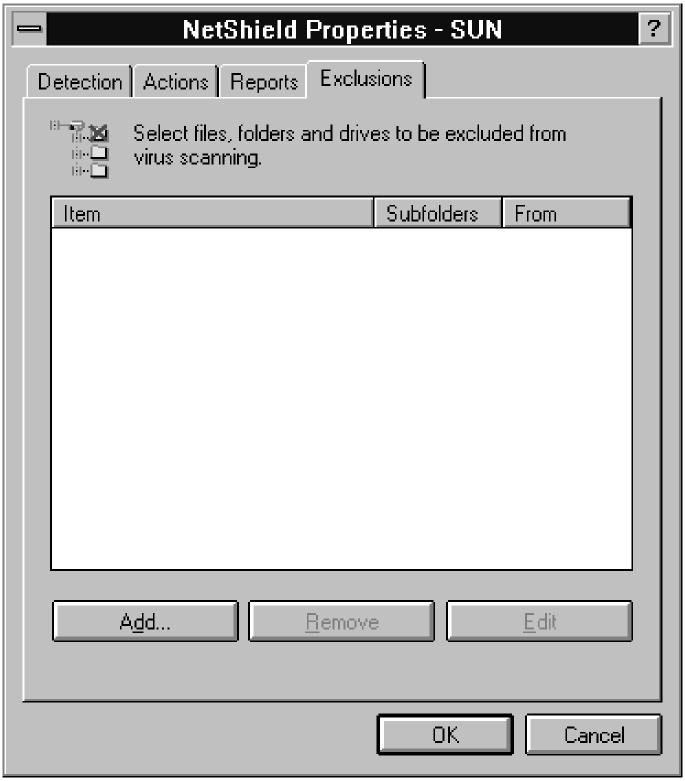

Select files, folders and drives to be excluded from virus scanning.

Figure 4-5. NetShield Properties Sheet (Exclusions Page)

2. Click Add to select folders to exclude from scanning.

   Response: The Exclude Item dialog box appears (Figure 4-6).

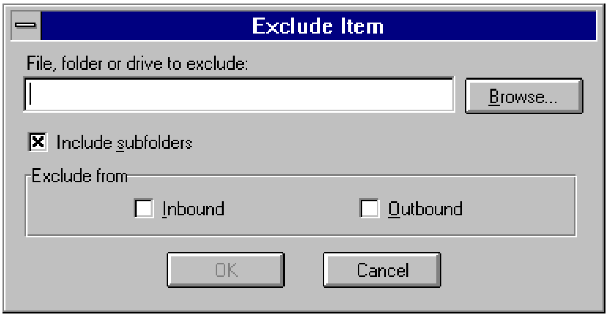


Figure 4-6. Exclude Item Dialog Box

3. Click Browse. Locate the folder to exclude and click OK.
4. To exclude subfolders, select the Include Subfolders checkbox, and click OK.
5. To exclude the item from Inbound and Outbound scanning, check the Inbound and Outbound checkboxes.
6. Repeat steps 2 through 5 until all items to be excluded are entered.
7. To edit an item, highlight the item and click Edit.
8. To delete an item, highlight the item and click Remove.
9. 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.

On-demand Tasks

Creating an on-demand task

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

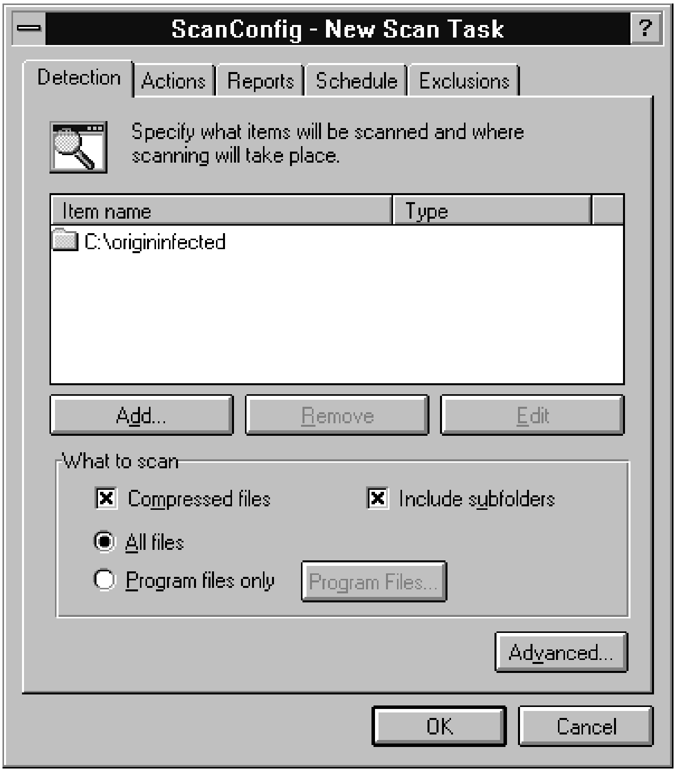
Response: A new on-demand task appears in the Console task window.

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 On-Demand Task.“

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

Response: The ScanConfig properties sheet appears with the Detection page displayed (Figure 4-7).



Specify what items will be scanned and where scanning will take place.

C:\origininfected

☒ Compressed files
☒ Include subfolders
● All files
○ Program files only

Figure 4-7. ScanConfig Properties Sheet (Detection Page)

Choosing file types and locations for scanning

To choose which files are scanned, complete the following procedure:

Step	Action
1.	Click the Detection tab of the ScanConfig properties sheet. **Response**: The Detection page appears (Figure 4-7).
2.	Click Add. **Response**: The Add Scan Item dialog box appears (Figure 4-8).

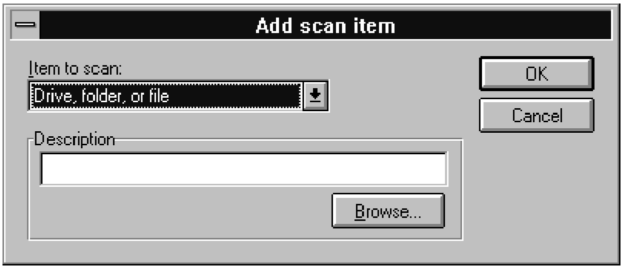
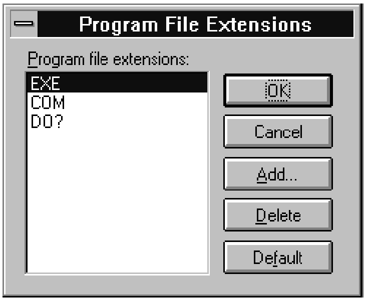


Figure 4-8. Add Scan Item Dialog Box

3. Select the location to scan:
   - To select an individual drive, folder, or file, select Drive, Folder, or File. Click Browse, select a folder to scan, and click OK.
   - To scan all drives, select All Local Drives.
4. To add more scanning locations, repeat steps 2 through 4.
5. Select the types of files to scan:
   - To scan all files, click the All Files option button. Skip to the next step.
   - To scan files with specific extensions, click the Program Files Only option button. Then click the Program Files button.

     Response: The Program File Extensions dialog box appears (Figure 4-9).



Program File Extensions

Program file extensions:

EXE
COM
DO?

Figure 4-9. Program File Extensions Dialog Box

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

6. To include compressed files, select the Compressed Files checkbox.

7. To include scanning of subfolders, select the Include Subfolders checkbox.

8. Click the Advanced button.

    - Set the priority level of the scan. High results in a fast scan with decreased network performance. Low extends the amount of time necessary to complete the scan.

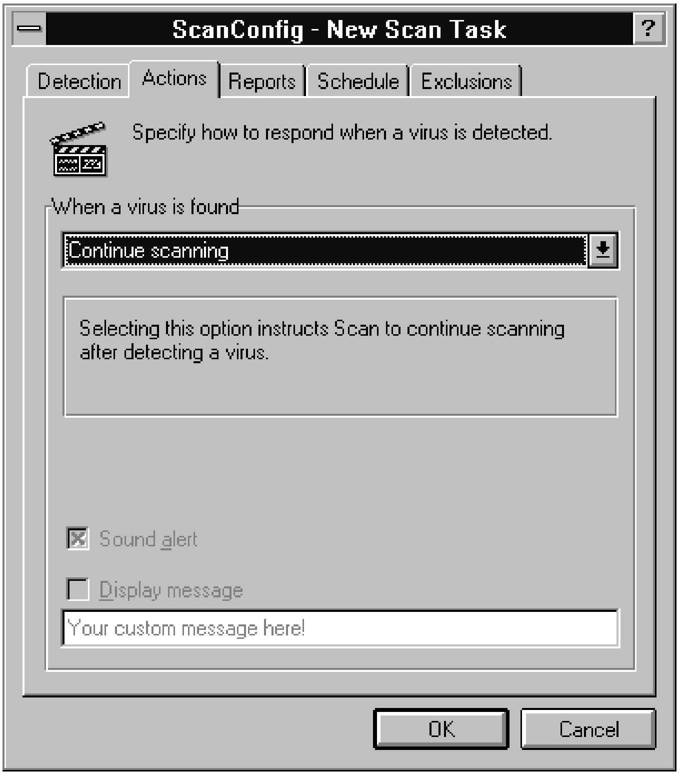
    - To skip boot record scanning, select Skip Boot Record Scanning.

9. 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.

Setting how NetShield responds to a virus infection

To control how NetShield responds to a virus detection, complete the following procedure:

Step	Action
1.	Click the Actions tab of the ScanConfig properties sheet. **Response**: The Actions page appears (Figure 4-10).



Specify how to respond when a virus is detected.

When a virus is found: Continue scanning

Selecting this option instructs Scan to continue scanning after detecting a virus.

☒ Sound alert

☐ Display message

Your custom message here!

Figure 4-10. ScanConfig Properties Sheet (Actions Page)

2. Select how NetShield responds to any viruses encountered. NetShield can respond by:

    - Cleaning the infected files
    - Deleting the infected files
    - Prompting you for action
    - Continuing Scanning

    If you select Prompt for Action, you should configure NetShield to send you an alert upon virus detection.

    - To configure NetShield to send you an audible alert upon virus detection, select the Sound Alert checkbox.
    - To configure NetShield to send you a custom alert message, select the Display Message checkbox and fill in the message.

3. 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.

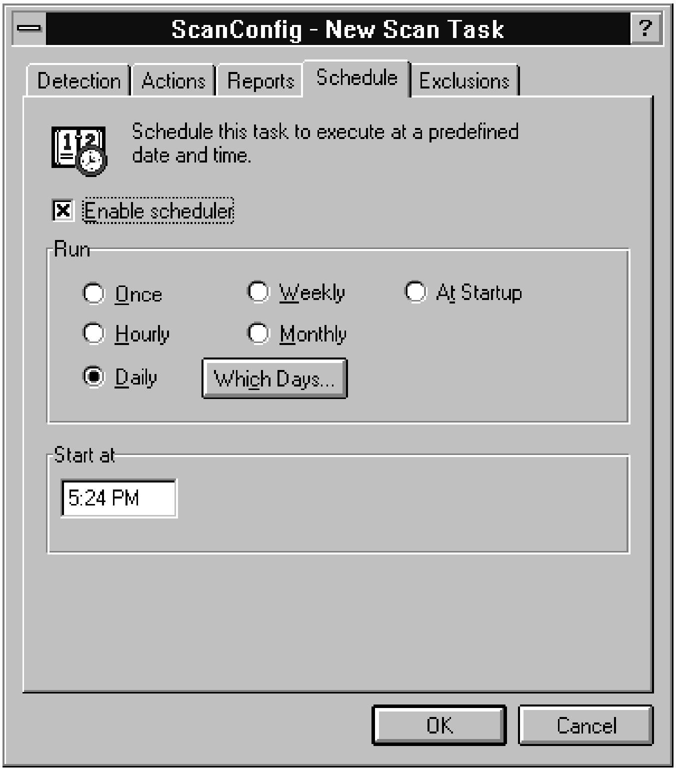
Scheduling the on-demand task

Decide how often the task will run. The task can be set to run:

- Once
- Hourly
- Daily
- Weekly
- Monthly
- Each time the server is started

To schedule a scan, complete the following procedure:

Step	Action
1.	Click the Schedule tab of the ScanConfig properties sheet. **Response**: The Schedule page appears (Figure 4-11).



Schedule this task to execute at a predefined date and time.

☒ Enable scheduler

Run

○ Once
○ Weekly
○ At Startup
○ Hourly
○ Monthly
● Daily

Start at

5:24 PM

Figure 4-11. ScanConfig Properties Sheet (Schedule Page)

2.	Select the Enable Scheduler checkbox.

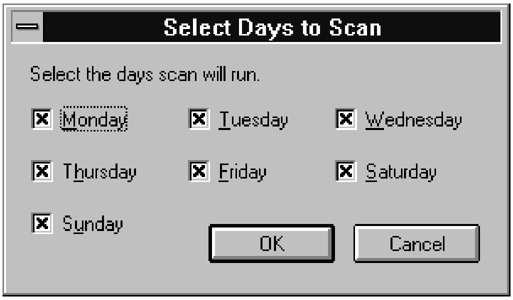
3. Select how often the task will run.

   - To schedule a one time scan, click the Once option button and enter the time and date.

   - To schedule an hourly scan, click the Hourly option button. Set the 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.

   - To schedule the scan for specific days, click the Daily option button. Enter the time for the scan to start, and click the Which Days button.

     Response: The Select Days to Scan dialog box appears (Figure 4-12).



Select the days scan will run.

☒ Monday ☒ Tuesday ☒ Wednesday
☒ Thursday ☒ Friday ☒ Saturday
☒ Sunday

Figure 4-12. Select Days To Scan Dialog Box

     Action: Choose which days the scan will run. Click OK.

   - To schedule a weekly scan, click the Weekly option button and enter the time and day of the week for the scan to start.

   - To schedule a monthly scan, click the Monthly option button and enter the time and day of the month for the scan to start.

   - To schedule a scan every time the server is started, click the At Startup option button.

4. Click OK.

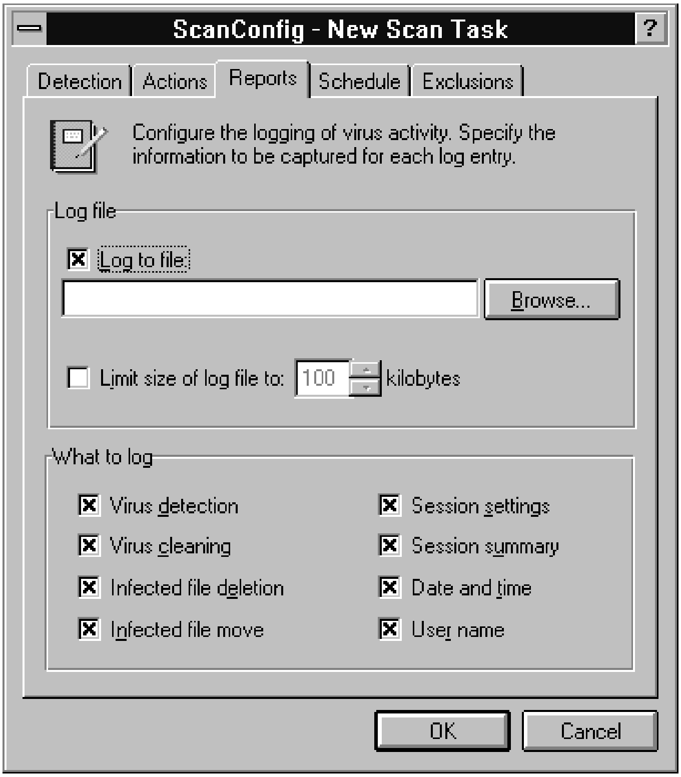
5. To further configure this task, select another dialog page. To save the changes and return to the Console, click OK. To cancel any changes and return to the Console, click Cancel.

Creating a virus activity log

The virus information log keeps track of all relevant NetShield activity, including virus detection, virus cleaning, infected file deletion, infected file move, and session settings.

To configure the log file, complete the following procedure:

Step	Action
1.	Click the Reports tab of the ScanConfig properties sheet. **Response**: The Reports page appears (Figure 4-13).



Configure the logging of virus activity. Specify the information to be captured for each log entry.

Log file

☒ Log to file:

☐ Limit size of log file to: 100 kilobytes

What to log

☒ Virus detection
☒ Virus cleaning
☒ Infected file deletion
☒ Infected file move
☒ Session settings
☒ Session summary
☒ Date and time
☒ User name

Figure 4-13. ScanConfig Properties Sheet (Reports Page)

2. Select the Log To File checkbox. To choose a new log file location, click Browse.

3. To limit the size of the log file, select the Limit Size checkbox and enter the maximum file size (in kilobytes).

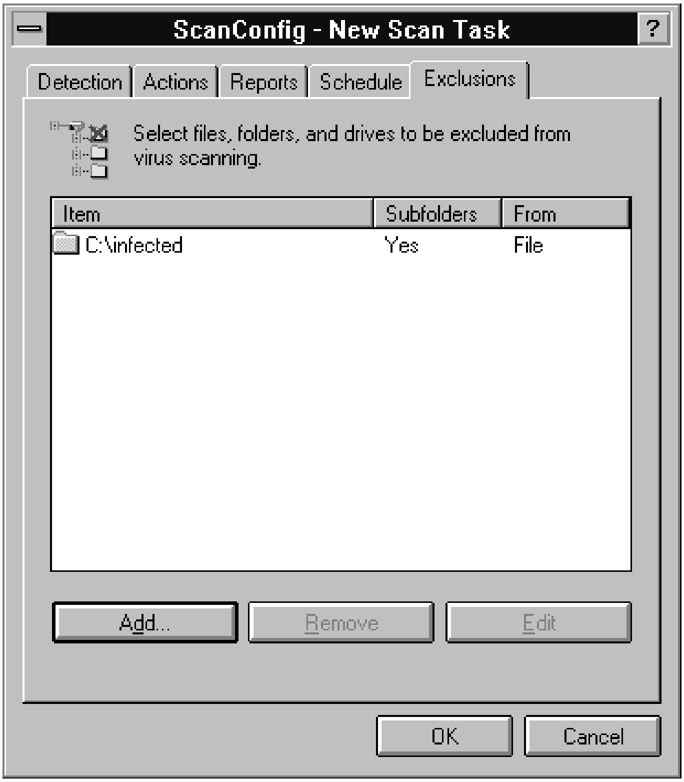
4. Choose the type of activity to include in the log file. To include a type of activity, select the activity's checkbox.

5. 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

To exclude files or folders from being scanned, complete the following procedure:

Step	**Action**
1.	Click the Exclusions tab of the ScanConfig properties sheet. **Response**: The Exclusions dialog page appears (Figure 4-14).



Select files, folders, and drives to be excluded from virus scanning.

Item	Subfolders	From
C:\infected	Yes	File

Figure 4-14. ScanConfig Properties Sheet (Exclusions Page)

2.	Click Add to select folders to exclude from scanning. **Response**: The Exclude Item dialog box appears (Figure 4-15).

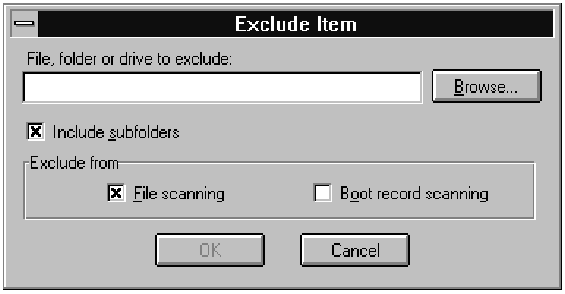


Figure 4-15. Exclude Item Dialog Box

3. Click Browse. Locate the file folder, or drive to exclude and click OK.

4. To exclude subfolders from scanning, select the Include Subfolders checkbox.

5. To exclude from file scanning or boot record scanning, check appropriate boxes.

6. Click OK.

7. Repeat steps 2 through 6 until all items to be excluded are entered.

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

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

10. 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.

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.

Working with 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 104.*

NetShield includes the IMPTASK utility for exporting VSC files to multiple servers. For more information, see "Using the IMPTASK utility" on page 44.

Exporting

To export a task, complete the following procedure:

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

To import a task, complete the following procedure:

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 OK.
	Response: The file is imported and appears as “New Scan Task” in the Console window.
4.	Enter a name for the new file. Click OK.
	Response: The ScanConfig properties sheet appears.
5.	Make any necessary changes to the task and click OK.

Copying and pasting tasks

To quickly configure multiple computers and save time, NetShield supports the copying and pasting of tasks. To copy a task, complete the following procedure:

Step	Action
1.	Highlight the task to copy and click 📋 or select Copy from the Edit menu.

2. Complete one of the following:

   - To copy the task to this computer, continue to the next step.
   - To copy the task to another computer, connect to the computer. For information on connecting to another computer, see "Changing Computers" on page 18.

3. Click 📋 or select Paste from the Edit menu.

   Response: The task is copied and appears as "New Scan Task" in the Console window.

4. Enter a name for the task and press ENTER.

   Response: The ScanConfig properties sheet appears.

5. Make any necessary changes to the task and 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 "Scheduling the on-demand task" on page 34.

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 20.

Deleting on-demand tasks

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

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
```

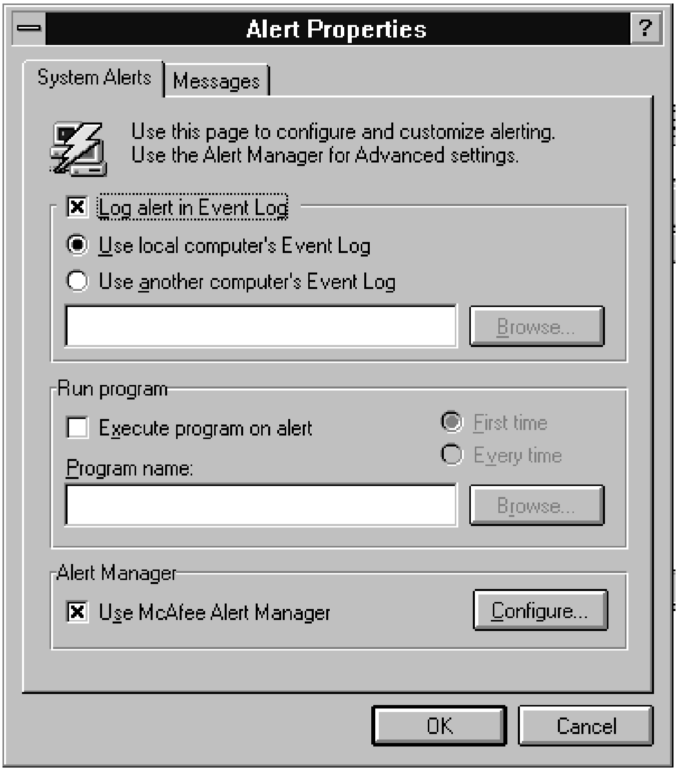
Imports the file YourTask.vsc to the computer named YourServer.

5

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 an event log, and alert personnel in a variety of ways (pagers, printers, e-mail, fax, etc.).

To open the Alert properties sheet, select Alerts from the Tools menu (Figure 5-1).



Use this page to configure and customize alerting.
Use the Alert Manager for Advanced settings.

☒ Log alert in Event Log
● Use local computer's Event Log
○ Use another computer's Event Log

Run program
☐ Execute program on alert
● First time
○ Every time
Program name:

Alert Manager
☒ Use McAfee Alert Manager

Figure 5-1. Alert Properties Sheet

Using Alert Manager

Use the Alert Manager to send alert notifications to computers, e-mail addresses, pagers, or printers.

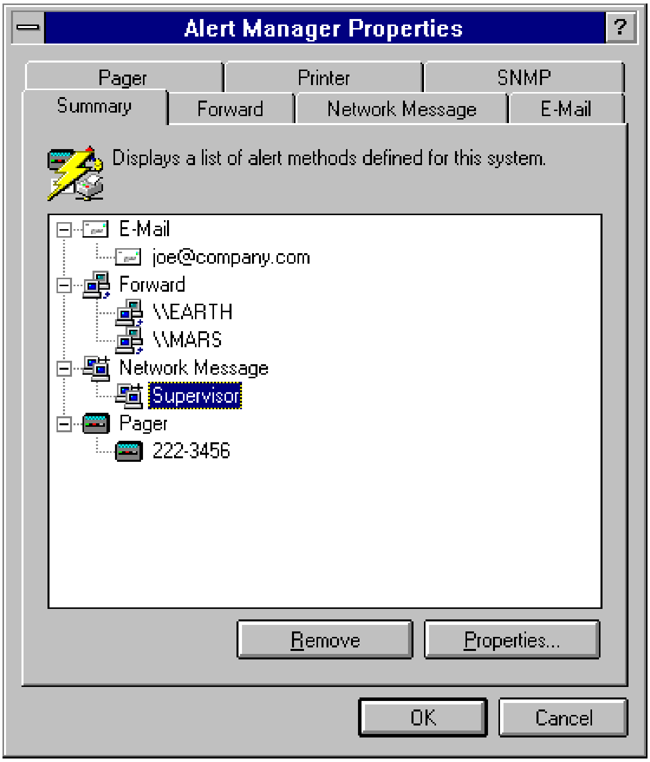
NetShield supports the use of any combination of notification methods and any multiples of each. To send additional alerts, use Forward to send alerts to another computer with the NetShield Console installed. When the computer receives a notification alert, it sends notifications to all of the recipients listed in its summary page.

✍ *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, complete the following procedure:

Step	**Action**
1.	Select Alerts from the Tools menu.
2.	From the System Alerts properties sheet, select Use McAfee Alert Manager checkbox and click Configure.

Response: The Alert Manager properties sheet appears with the Summary page showing (Figure 5-2).



Displays a list of alert methods defined for this system.

- E-Mail
  - joe@company.com
- Forward
  - \\EARTH
  - \\MARS
- Network Message
  - Supervisor
- Pager
  - 222-3456

Figure 5-2. Alert Manager Properties Sheet

Summary page

The Summary page lists all alert notification items configured on the other properties pages.

- To view the properties of a notification item, highlight the item and click Properties.
- To delete a notification item, highlight the item and click Remove.

Forwarding alerts to another computer

NetShield can forward alerts to another computer. The computer receiving the forwarded message then sends alerts to recipients listed in the Summary page of its Alert Manager properties sheet.

✍ *The McAfee Alert Manager Service must be running on both the system sending the Forward and the system receiving it.*

Step **Action**

1. Open the Alert Manager properties sheet.

2. Select the Forward tab.

   Response: The Forward page appears with a list of all systems configured to receive forwarded messages.

3. To add a computer to receive Forwards, click Add.

4. Specify a computer or click Browse to locate the computer.

5. To test the forward, click Test.

   Response: The computer receives a test message.

6. To set the priority level of the messages this forward receives, click Priority Alerts.

   - To set the address to receive low, medium, and high priority alerts, select Low.

   - To set the address to receive medium and high priority alerts, select Medium.

   - To set the address to receive high priority alerts only, select High.

   ✍ *Configure High Priority items to be forwarded to other computers. This increases the number of alert notifications sent in an urgent situation and improves the chances of someone responding to the problem quickly.*

7. Click OK.

8. To add another computer to receive forwarded alerts, click Add.

9. To configure other notification options, select another properties page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

✍ *The NetShield Console must be installed and running on the computer receiving forwarded messages.*

Sending a network message

The Alerts Manager supports the sending of network messages to specified computers. To send alert notifications via network messages, complete the following procedure:

✍ *To receive messages on Windows 95 machines, you must be running WinPopup.*

Step **Action**

1. Open the Alert Manager properties sheet.

2. Select the Network Message tab.

   Response: The Network Message page appears with a list of all systems configured to receive network messages.

3. To add a system to receive network message alert notifications, click Add.

4. Enter the computer to receive network messages or click Browse to locate the computer.

5. To test the connection, click Test.

   Response: The message recipient receives a test message.

6. To set the priority level of the messages this computer receives, click Priority Alerts.

   - To set the system to receive low, medium, and high priority alerts, select Low.
   - To set the system to receive medium and high priority alerts, select Medium.
   - To set the system to receive high priority alerts only, select High.

7. Click OK.

8. To add another system to receive network message alert notifications, click Add.

9. To configure other notification options, select another properties page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

Sending an alert to an e-mail address

The Alerts Manager supports the sending of e-mail messages. To send alert notifications via e-mail, complete the following procedure:

Step	Action
1.	Open the Alert Manager properties sheet.
2.	Select the E-Mail tab. **Response**: The E-Mail page appears with a list of e-mail addresses configured to receive alert notifications.

3. To add an e-mail address, click Add.

   Enter an e-mail address. The format of the address is <user>@<domain> (e.g. johndoe@mcafee.com).

   Fill out the Subject line

   Fill out the From line.

4. To configure SMTP settings, click Configure SMTP, enter the Domain name or IP address, Server name, and Login name.

5. To test the connection, click Test.

   Response: The message recipient receives a test message.

6. To set the priority level of the messages this e-mail address receives, click Priority Alerts.

   - To set the address to receive low, medium, and high priority alerts, select Low.
   - To set the address to receive medium and high priority alerts, select Medium.
   - To set the address to receive high priority alerts only, select High.

7. Click OK. To add another recipient to receive alert notifications, click Add.

8. To configure other notification options, select another properties page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

Sending an alert to a pager

The Alerts Manager supports the sending of alert notifications to alphanumeric and numeric pagers.

Alphanumeric pager

To send alert notifications to an alphanumeric pager, complete the following procedure:

Step	**Action**
1.	Open the Alert Manager properties sheet.
2.	Select the Pager tab.
	Response: The Pager page appears with a list of all pagers configured to receive alert notifications.
3.	To add a pager, click Add.
4.	Select Alphanumeric Pager.
5.	Enter the pager phone number, an ID or a PIN number (if applicable), and a password (if applicable).
6.	To use the standard alert message, click the Use Standard Alert Message option button.
	To use a custom message, click the Use Custom Alert Message option button and enter a message.
7.	Click Modem to configure the modem settings.
8.	To test the pager, click Test.

9. To set the priority level of alert notifications this pager receives, click Priority Alerts.

   - To set the address to receive low, medium, and high priority alerts, select Low.

   - To set the address to receive medium and high priority alerts, select Medium.

   - To set the address to receive high priority alerts only, select High.

10. Click OK.

11. To add another pager to receive notifications, click Add.

12. To configure other notification options, select another properties page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

Numeric pager

To send alert notifications to an numeric pager, complete the following procedure:

Step **Action**

1. Open the Alert Manager properties sheet.

2. Select the Pager tab.

   Response: The Pager page appears with a list of all pagers configured to receive alert notifications.

3. To add a pager, click Add.

4. Select Numeric pager.

5. Enter the pager phone number.

6. Enter a numeric message.

7. Enter the delay time between dialing and sending the alert message.

8. Click Modem to configure the modem settings.

9. To test the pager, click Test.

10. To set the priority level of alert notifications this pager receives, click Priority Alerts.

    - To set the address to receive low, medium, and high priority alerts, select Low.

    - To set the address to receive medium and high priority alerts, select Medium.

    - To set the address to receive high priority alerts only, select High.

11. Click OK.

12. To add another pager to receive notifications, click Add.

13. To configure other notification options, select another properties page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

Sending an alert to a printer

The Alerts Manager supports the sending of alert notifications to printers. To send alert notifications to printers, complete the following procedure:

Step	Action
1.	Open the Alert Manager properties sheet.
2.	Select the Printer tab. **Response**: The Printer page appears with a list of all systems currently configured to receive alert notifications.
3.	To add a printer, click Add.

4. Enter a printer location or click Browse to locate the printer.

5. To test the connection, click Test.

   Response: The printer prints a test message.

6. To set the priority level of the messages this printer receives, click Priority Alerts.

   - To set the system to receive low, medium, and high priority alerts, select Low.
   - To set the system to receive medium and high priority alerts, select Medium.
   - To set the system to receive high priority alerts only, select High.

7. Click OK.

8. To add another printer to receive alert notifications, click Add.

9. To configure other notification options, select another properties page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

✍ *The printer must be configured by the Print Manager prior to configuring this notification option.*

Using SNMP

NetShield supports SNMP (Simple Network Management Protocol). To enable SNMP, complete the following procedure:

Step **Action**

1. Open the Alert Manager properties sheet.

2. Select the SNMP tab.

   Response: The SNMP page appears.

3. Select the Enable SNMP checkbox.

4. To configure SNMP services, click Configure.

   Response: The Microsoft NT Network Settings properties sheet appears.

5. To complete configuration of SNMP services, refer to the Windows NT documentation.

6. To configure other notification options, select another properties page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

Executing a Program on Alert

In the event Alert Manager does not meet your needs, it may 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 McAfee, you could write a batch file to send notifications to your mail package.

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

To configure NetShield to execute a program on alert, complete the following procedure:

Step	**Action**
1.	Select Alerts from the Tools menu.
2.	Select the Execute Program on Alert checkbox.
3.	Enter the name and path of the program to execute or click Browse to locate the program.
4.	To execute the program every time an alert event occurs, click the Every Time option button. To execute the program on the first alert event only, click the First Time option button.
5.	To save the changes and return to the console, click OK. To cancel any changes, click Cancel.

Logging Alerts

To configure NetShield to log alerts in the Windows application log, complete the following procedure:

Step	Action
1.	Select Alerts from the Tools menu.
2.	Select the Log Alert in Event Log checkbox.
3.	To log alert events in the local computer’s event log, click the Use Local Computer’s Event Log option button.
4.	To log alert events in another computer’s event log, click the Use Another Computer’s Event Log option button. Click Browse to locate the computer.
5.	Click OK.
	Response: Alert events are stored in the Event Log.

✍ *To open the application log, click or select Event Log from the Tools menu.*

Customizing Alerts

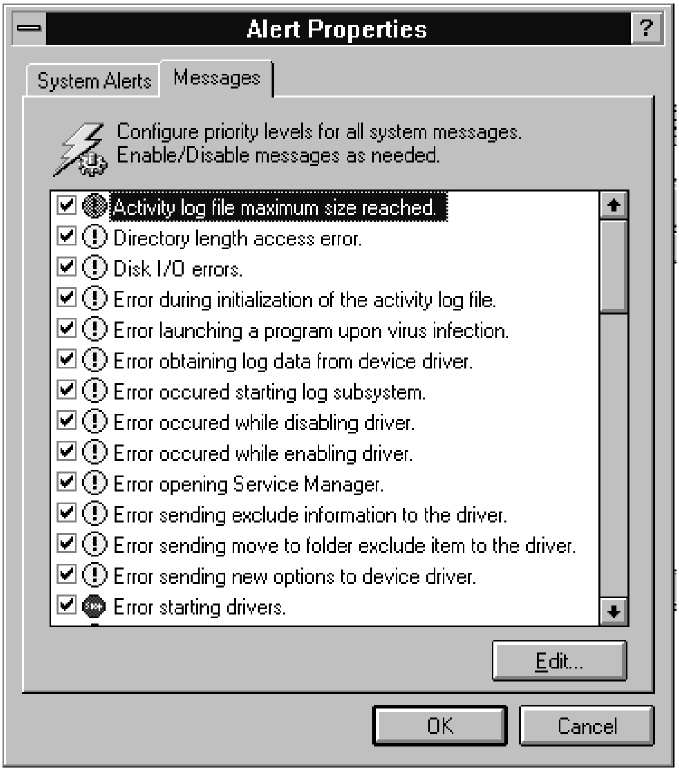
Enabling/disabling alerts

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 5-3).



Configure priority levels for all system messages.
Enable/Disable messages as needed.

- ☑ Activity log file maximum size reached.
- ☑ Directory length access error.
- ☑ Disk I/O errors.
- ☑ Error during initialization of the activity log file.
- ☑ Error launching a program upon virus infection.
- ☑ Error obtaining log data from device driver.
- ☑ Error occured starting log subsystem.
- ☑ Error occured while disabling driver.
- ☑ Error occured while enabling driver.
- ☑ Error opening Service Manager.
- ☑ Error sending exclude information to the driver.
- ☑ Error sending move to folder exclude item to the driver.
- ☑ Error sending new options to device driver.
- ☑ Error starting drivers.

Figure 5-3. Alert Properties Sheet (Messages Page)

2. To enable an alert, select its checkbox.

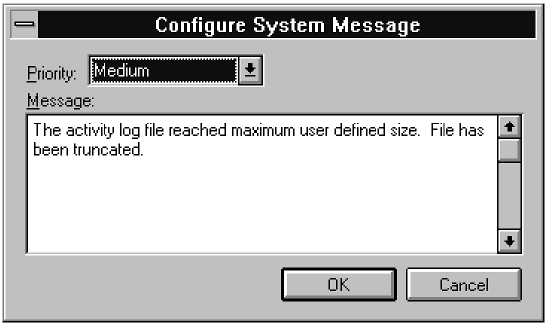
3. To disable an alert, deselect its checkbox.

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, complete the following procedure:

Step	Action
1.	Select Alerts from the Tools menu and click the Messages tab. **Response**: The Alert properties sheet appears (Figure 5-3) with the Messages page displayed.
2.	Highlight an alert and click Edit. **Response**: The Configure System Message dialog box is displayed (Figure 5-4).



Priority: Medium

Message:

The activity log file reached maximum user defined size. File has been truncated.

Figure 5-4. Configure System Message Dialog Box

3.	Select a priority level.
4.	Click OK.

Customizing an alert message

To customize an alert message, complete the following procedure:

✍ *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.*

Step	**Action**
1.	Select Alerts from the Tools menu and click the Messages tab.
	Response: The Alert properties sheet appears (Figure 5-3) with the Messages page displayed.
2.	Highlight an alert and click Edit.
	Response: The Configure System Message dialog box is displayed (Figure 5-4).
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

6

Updating NetShield

Overview: AutoUpdate

Approximately once a month, McAfee updates NetShield to add new virus detectors, add new options, and fix reported bugs. To distribute these new versions, a multi-line bulletin board system, a forum on CompuServe, and an Internet node are available.

AutoUpdate is a powerful feature that can ensure you always have the latest version of the anti-virus data files on your systems. AutoUpdate can automatically download updates from an ftp site or network distribution site. After the update is downloaded, AutoUpdate can post the update to a distribution site for downloading by other computers.

✍ *Obtaining updates from outside the network typically requires the writing of a shell script. The script included with NetShield is only a sample and must be modified to suit your needs.*

How AutoUpdate works

When AutoUpdate runs, it looks for a file named VERSION.DAT. This file contains the following information:

[NETSHIELD]	Designates the product to which this file applies.
uVersion=X	X is the version of the new update.
uVersionreq=Y	Y is the version required to use this update
szUpdateModule=FILENAME	FILENAME is the name of the file which will be retrieved and executed.

When AutoUpdate locates VERSION.DAT, it determines whether the update is needed and if your version of NetShield is current enough to use the update.

- If the update is not required, AutoUpdate sends you a No Update Required message.
- If your version of NetShield is not current enough to use the update, AutoUpdate informs you that you need to upgrade your version of NetShield to qualify for the update. To upgrade your version, visit the McAfee Web Site. See "How To Contact Us" on page 9.
- If the update is needed, AutoUpdate executes the file specified by VERSION.DAT.

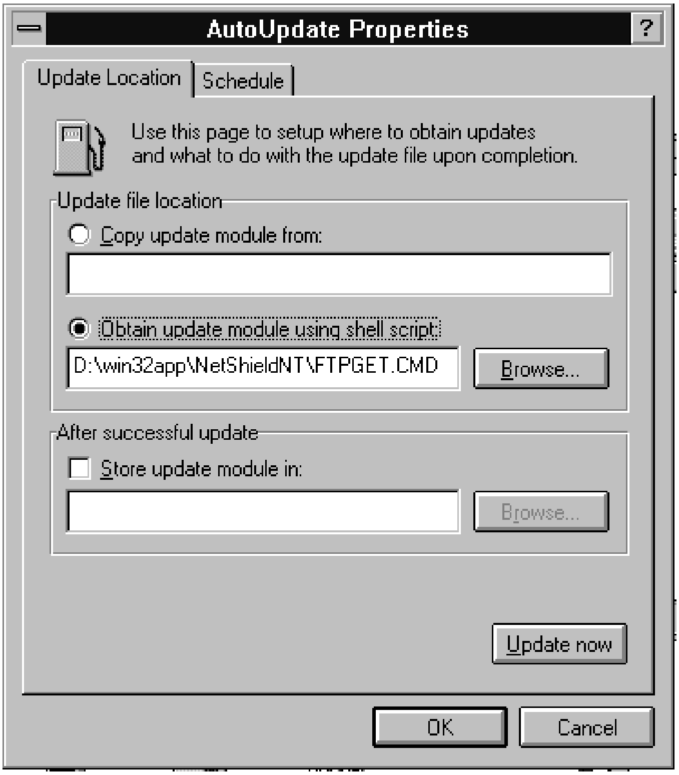
Obtaining an Update

To obtain an update using AutoUpdate, complete the following procedure:

Step **Action**

1. Select AutoUpdate from the Tools menu.

Response: The AutoUpdate properties sheet appears with the Update Location page displayed (Figure 6-1).



Use this page to setup where to obtain updates and what to do with the update file upon completion.

○ Copy update module from:

● Obtain update module using shell script:

D:\win32app\NetShieldNT\FTPGET.CMD

☐ Store update module in:

Figure 6-1. AutoUpdate Properties Window

2. Complete one of the following steps:

   - To obtain the update using a shell script, click the Obtain Update Module Using Shell Script option button. Enter the location of the shell script or click Browse to choose a location.

   - To obtain the update from a distribution site, click the Copy Update Module From option button. Enter the full path to the location of the update module and VERSION.DAT.

3. After AutoUpdate downloads an update, it can store a copy of the update on a distribution site for other computers to access.

   To upload the update module to a distribution site, select the Store Update Module In checkbox. Enter a location for the distribution site or click Browse to choose a location.

4. Complete one of the following steps:

   - To perform the update now, click Update Now.

     Response: AutoUpdate begins downloading the latest update. Once the update is complete, click OK to return to the Console.

   - To schedule AutoUpdate, click the Schedule tab.

     Response: The Schedule page appears. Continue to the next step.

5. Select when or how often AutoUpdate will update its data files. When finished, click OK to save the configuration and return to the Console.

   ✍ *If you selected Daily, be sure to specify which days you want the update to occur. To select the days, click Which Days.*

Creating a Script

Obtaining updates from outside your network typically requires you to create a script. Once created, AutoUpdate can be configured to execute the script automatically.

✍ *This section will not teach you how to write a script. If you do not know how to write a script, consult a programmer.*

The sample script works by creating a temporary file, which contains the parameters required by ftp to obtain the update. These include the ftp site name, the user name, the binary file transfer, the file %1 (%1 is either VERSION.DAT or the update filename, as specified by AutoUpdate), and the quit parameters.

This following script is notated with information explaining the function of each line.

✍ *This script will not work without modification.*

```
@echo off
rem *****  FTPGET.CMD                                 *****
rem *****  Copyright (C) 1996 McAfee Associates Inc.  *****
rem *****  This script will download file specified   *****
rem *****  on the command line from mcafee.com        *****
rem *****  /pub/updates directory                     *****
rem *****  errors and status information will be      *****
rem *****  logged into FTPGET.LOG in the current      *****
rem *****  directory                                  *****

rem Create FTP command file FTPCMD.FTP
echo open>FTPCMD.FTP
```

Creates the file FTPCMD.FTP and adds “open” to the file.

```
echo ftp.mcafee.com>>FTPCMD.FTP
```

Adds the ftp site name to FTPCMD.FTP.

```
echo ftp>>FTPCMD.FTP
```

Adds the ftp command to FTPCMD.FTP.

```
echo %USERNAME%@%USERDOMAIN%>>FTPCMD.FTP
```

Adds the user name needed to log on to the site to FTPCMD.FTP.

```
echo bin>>FTPCMD.FTP
```

Adds bin to FTPCMD.FTP. Indicates binary file transfer.

```
echo get /pub/updates/%1>>FTPCMD.FTP
```

Adds the filename to get to FTPCMD.FTP. Passed as %1 by AutoUpdate.
The update path is subject to change. Contact McAfee for the latest update location.

```
echo close>>FTPCMD.FTP
```

Closes the file FTPCMD.FTP.

```
echo quit>>FTPCMD.FTP
```

Closes the ftp connection.

```
rem Now launch ftp.exe with the command file FTPCMD.FTP
ftp -s:FTPCMD.FTP >> FTPGET.LOG
```

Launches FTP.EXE with the appropriate command line parameters configured in FTPCMD.FTP.

```
rem Now delete FTPCMD.FTP
del FTPCMD.FTP > nul
```

Deletes FTPCMD.FTP.

```
rem We're done
```

The update is download and the ftp session is closed.

A

Encountering Viruses

Don’t Panic!

This chapter explains what to do when you have or suspect you have a virus infection.

- If you downloaded or purchased this program because you suspect you have a virus or if NetShield prompts you to shut down your system, see “If You Have or Suspect You Have a Virus” on page 70.
- If NetShield or Scan prompts you to remove a virus, see “Removing Viruses at NetShield’s prompt.” on page 73.

If You Have or Suspect You Have a Virus

If you suspect your system is infected with a virus prior to installing NetShield or if NetShield or Scan32 encounters a virus and prompts you to shut down your system, complete one of the following procedures:

- If you can get into the system, see “If you can get into the system,” following.
- If you cannot get into the system, see “If you cannot get into the system” on page 71.

If you can get into the system

✍ *Due to the nature of some viruses, it may not be possible to restart your system once the viruses are removed. If you can get into your system, it is highly recommended to perform a backup prior to using the Emergency Disk.*

Step	**Action**
1.	Backup your system using a fresh tape.
2.	Shut down the system.
3.	Place the Emergency Disk in the A: drive. ✍ *Make sure the BIOS is set to boot from the A: drive first.*
4.	Turn the computer on.

5. Follow the on-screen instructions and remove any viruses found.

    - If the Emergency Diskette removes the viruses, continue to the next step.

    - If Emergency Diskette does not remove the viruses, use the McAfee Website to find information on manually removing viruses. See “How To Contact Us” on page 9.

    ✍ *If you are using a NTFS (New Technologies File System) partition, it will not be visible to the Emergency Disk. This procedure only eliminates viruses on the Master Boot Record (MBR) or boot sector of visible DOS partitions.*

6. Restart the system.

7. Install NetShield. For information on installing NetShield, see “Performing the Installation” on page 13.

8. Run Scan32 on all drives. See “Using Scan32” on page 81.

If you cannot get into the system

If you cannot get into the system, it may be helpful to use the Windows NT Installation Diskettes with the Emergency Disk created by Microsoft’s RDISK utility. To repair the system area, complete the following procedure:

Step **Action**

1. Turn the machine off.

2. Insert the Windows NT Installation diskette into the A: drive.

    ✍ *If you do not have these diskettes or did not create the Emergency diskette with the RDISK utility, you can try scanning the system with a generic boot diskette. To create one, format a diskette on another Windows NT machine and copy the following files: NTDETECT.COM, NTLDR.COM, BOOT.INI, AND NTBOOTDD.SYS (SCSI systems only).*

3. Start the system.

4. Follow the instructions for repairing a Windows NT installation.

5. Restart the system.

   - If the system restarts, see “If you can get into the system” on page 70.

   - If the system doesn’t restart, continue to the next step.

6. Reinstall Windows NT.

7. Load the most recent backup files.

8. Run Scan32 on all drives. See “Using Scan32” on page 81.

Removing Viruses at NetShield’s prompt.

NetShield and Scan32 offer a variety of cleaning options. If NetShield or Scan32 prompts you to remove a virus, complete the following procedure:

Step **Action**

1. Select how to respond to the virus infection.

- To clean the file or remove the virus from the file, click Clean.
- To delete the file, click Delete.

  ✍ *Note the filename and path to restore the file from backups. To configure NetShield or Scan32 to automatically keep track of deleted files, select the Log To File option. For NetShield, see “Creating a virus activity log” on page 37. For Scan32, see “Using Scan32” on page 81.*

- To move the infected file to a quarantine folder, click Move File To and select a location.
- To continue scanning without taking any action, click Continue.

  ✍ *This option is not recommended.*

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

✍ *If NetShield or Scan32 cannot clean a virus, run Scan32 again, delete the infected files, and restore them from backups. For more information, see “Using Scan32” on page 81.*

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 33.

4. To find and eliminate the source of the infection, scan your diskettes immediately. For information about scanning diskettes, see “Scanning Your Diskettes” on page 75.

B

Preventing Virus Infection

This chapter contains various procedures for maintaining a safe computing environment. These include:

- Scanning Your Diskettes
- Write Protecting a Diskette
- Updating Data Files

Scanning Your Diskettes

Although the on-access scanning component of NetShield will monitor your system for viruses, it is recommended to scan all diskettes you use on your PC. Most viruses invade your system when you either start your system with an infected diskette in the A: drive or copy, run, or install programs that contain infected files.

Always make sure your diskette drives are empty before turning on your computer. A diskette does not have to be bootable in order to catch a boot sector virus.

When should I scan diskettes?

Scan all diskettes that you do not know to be virus-free before executing, installing, or copying files. This includes diskettes received from friends, co-workers, salespeople, and even your own diskettes (if they have been used on another PC).

How do I scan my diskettes?

Use the procedures below to scan your diskettes after NetShield is installed.

Step	Action
1.	Launch NetShield by double-clicking the NetShield icon in the McAfee NetShield program group.
2.	Click the Select icon.
	Response: The Select Items to Scan dialog box is displayed.
3.	Select the A: drive from the Drives list, then choose Add Drive.
	Response: The A: drive is displayed in the Selections list.
4.	Click OK to return to the NetShield Main Window.

5. Insert a diskette and click Scan.

   Response: The diskette is scanned and the names of any infected files found are displayed.

6. Complete one of the following:

   - If NetShield doesn’t find a virus on the diskette, continue to the next step.

   - If NetShield finds a virus, select one of the cleaning options.

7. Repeat this procedure for all diskettes normally used.

Write Protecting a Diskette

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

One way to help avoid infection via floppy diskette is to *write protect* the diskettes you are using for read-only data. Write protecting diskettes prevents data from being written to them.

If your system does become infected with a virus, this feature keeps your clean diskettes from becoming infected and prevents reinfection after your system is cleaned.

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

Step	**Action**
1.	Position the diskette face down with the metal slide facing you. Examine the small rectangular hole on the upper left side. There should be a square, plastic tab that you can slide up and down across the hole.
2.	To write protect the diskette, slide the plastic tab upward toward the corner of the diskette so the hole is open.

Updating Data Files

New viruses (and variants of old ones) are constantly appearing and circulating throughout the personal computer community. McAfee updates the programs regularly—usually monthly, but sooner if many new viruses appear. Each new version detects and removes as many as 60 to 100 new viruses, and may add new features to the NetShield product. To find out what's new, read the WHATSNEW.TXT text file that shipped with this product.

Download new versions

You can download evaluation copies of new versions of McAfee products from the McAfee Website. For more information, see "How To Contact Us" on page 9. New versions of McAfee software are stored in compressed form to reduce transmission time.

To update your virus definition data, complete the following steps:

Step	Action
1.	Create a new directory for the downloaded file.
2.	Copy the file to the new directory.
3.	Unzip the file. ▪ Double-click the file. **Response**: The WinZip dialog box is displayed. **Action**: Click Extract. **Response**: The files are unzipped.

✍ *If the files do not unzip and the procedure does not work properly, see the McAfee Web Site for information on downloading and using Pkunzip and WinZip. For information about the McAfee Web Site, see "How To Contact Us" on page 9.*

4. Copy the files NAMES.DAT, CLEAN.DAT, and SCAN.DAT to the appropriate directory. Occasionally SCAN32.EXE is updated. If there is a new version of SCAN32.EXE, copy it to the directory as well. The default directory location is shown below.

   x:\Win32App\NetShield NT (NT 3.5)

   X:\Program Files\McAfee\NetShield NT (NT 4.0)

✍ *Always download and decompress the files in a separate directory from your current files.*

5. Before performing any scans, shut down your computer, wait a few seconds, and turn it on again. NetShield may report a “failed integrity check” if you attempt a scan immediately after an update.

Validate the program files

When you download a program file from any source other than the McAfee bulletin board or other McAfee service, it is important to verify it is authentic, unaltered, and uninfected. McAfee anti-virus software includes a program called Validate, which ensures your version of NetShield is authentic. When you receive a new version of NetShield, follow Validate’s instructions to ensure successful verification of all program files. See README.1ST for more information on the Validate program.

C

Using Scan32

What is Scan32?

Scan32 is an independent software program that complements the NetShield Console. The NetShield Console automates the process of scanning and is ideal for implementing long-term anti-virus strategies. Scan32 offers a quick way to scan for viruses now.

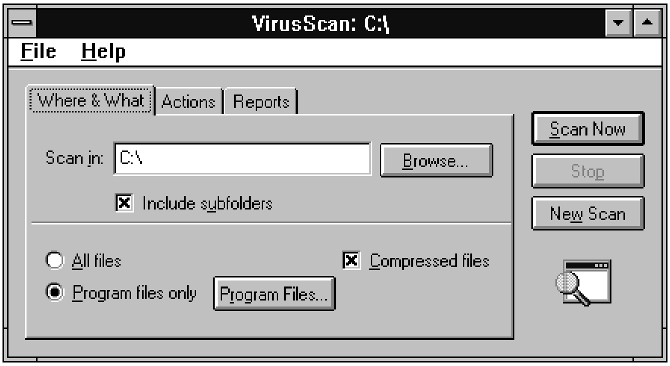
Using Scan32

To scan for viruses using Scan32, complete the following procedure:

Step **Action**

1. From the Windows NT Program Manager, open the McAfee NetShield group and double-click the Scan32 icon.

Response: The Scan32 properties sheet is displayed with the Where & What page showing.



Scan in: C:\

☒ Include subfolders

○ All files

● Program files only

☒ Compressed files

Figure C-1. Scan32 Properties Sheet (Where & What Page)

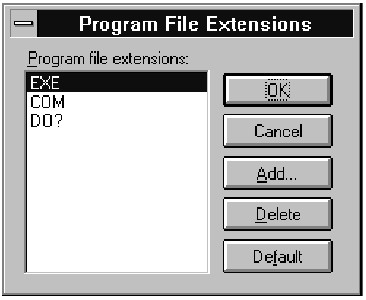
2. Enter a location to scan or click Browse to choose a location.

3. To include scanning of subfolders, select the Include Subfolders checkbox.

4. Select the types of files to scan:

- To scan all files, click the All Files option button. Skip to the next step.
- To scan files with specific extensions, click the Program Files Only option button. Then click the Program Files button.

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



Program File Extensions

Program file extensions:

EXE
COM
DO?

Figure C-2. Program File Extensions Dialog Box

- To add a file extension to scan, click Add. Enter the new file extension and click OK.
- 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.

5. To include compressed files, select the Compressed Files checkbox.

6. Click the Action tab.

   Response: The Action properties page appears.

7. Select how Scan32 will respond to viruses:

   - Scan32 prompts you for action.
   - Scan32 automatically cleans any infected files.
   - Scan32 automatically deletes any infected files.

   If you select automatic deletion of infected files, make sure to select the Log To File checkbox. When Scan32 finishes deleting infected files, you can look them up in the log file and restore them from backups.

- Scan32 moves the infected files to a folder.
- Scan32 continues scanning without taking any action.

  ✍ *This option is not recommended.*

8. To begin scanning, click Scan Now. To exit without scanning, click Cancel.

Reporting options

To configure Scan32's reporting options, complete the following procedure:

Step **Action**

1. Click the Reports tab of the Scan32 properties sheet.

2. To display a custom message, select the Display Custom Message checkbox and enter a message.

✍ *For Scan32 to display a custom message, the Prompt for Action option must be selected on the Action page.*

3. For an audible alert, select Sound Alert.

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

To limit the size of the log file, select the Limit Size checkbox and enter the maximum size.

5. To begin scanning, click Scan Now. To exit without scanning, click Cancel.

D

Understanding Viruses

Computer Virus Primer

Your computer posted an unusual message, changed screen colors, is missing files, has no hard disk space left, or just plain won't work. Is this a virus? In many cases, the answer is no. These are all symptoms of viruses and viral damage. However, the problems actually may be caused by a faulty system battery, keyboard error, someone else's misuse, a practical joke, fragmented disks, or even reboot corruption. Unless you use anti-virus software, it is difficult to determine if computer anomalies are caused by viruses.

Typical Signs of Virus Infection

- Unusual messages
- Missing files or increased file size
- Slow system operation
- No more disk space
- No more disk access

Every month, more than 100 new viruses are added to the worldwide viral pool of more than 8,500. The threat from these viruses is real. According to a National Computer Security Association March 1996 survey of 2,300 North American companies with 500 or more PCs:

- Approximately 90% of companies experience a virus encounter or incident each month.

- Approximately 90% believe that the virus problems are the same as or worse than last year.

- The Word.Concept macro virus appears to be the fastest growing virus and seems to travel to a large extent by e-mail and other network connections.
- Virus encounters average 1 per 100 PCs per month.
- Over 70% of infections occur through diskette distribution.
- More than 80% of infections result in lost productivity, and 35% result in lost data.
- Over 46% of infections require more than 19 days for complete recovery.
- More than 35% of incidents cost $2,000 or more.
- Less than 35% of companies use the full-time protection capabilities of their anti-virus software.
- Over 20% of viruses reported were received due to electronic distribution.
- The average server virus incident takes over 5.5 hours for recovery.

What is a virus?

The classic definition of a computer virus is a program that replicates itself, attaches to other programs, and performs unsolicited, if not malicious, actions when executed.The two fundamental virus categories are “boot” and “file” viruses.

Boot viruses are programs that become active upon system start-up. They dwell within the boot sector of a system’s infected floppy or hard disk. Most often, the boot virus spreads as it becomes memory resident, replicating and attaching onto other available logical disks. Subsequent use allows the virus to spread to other disks.

File viruses are programs that become active only when executed—these include .exe, .com, .dll and other executable files. The file virus spreads upon execution as it typically becomes memory resident, then replicates and attaches to other executable programs.

Other viral classifications also exist. *Multi-partite viruses*, for example, are viruses that have both file and boot virus characteristics. *Stealth viruses* hide their actions either generically or against specific anti-virus products. *Encrypted viruses* actually encrypt their viral code, further hiding from detection. *Polymorphic viruses* use mutation engines to randomize their signature. Today, the most common widespread virus is a new classification called a *macro virus*. Macro viruses use an application's macro language to spread to other documents within that application and perform unsolicited actions. The Word macro virus is obtained by opening macro-infected Microsoft Word document (.doc) or Word template (.dot) files.

How do viruses spread?

Incident reports indicate that the majority of viruses are introduced innocently to end-user environments from unsuspecting employees, family, and friends. Depending on a site's software security standards, it is even possible to contract a computer virus when sending your PC to a repair service center, utilizing re-packaged software or using new software.

How One Receives A Computer Virus

- Diskette and file sharing
- File exchange from e-mail, online services, the Internet, and bulletin board systems
- Re-packaged software and repair services.

It is not uncommon to believe that you just received a computer virus and it caused immediate damage. Today's computer viruses, however, are designed to spread among computers before causing enough damage to evoke publicity. If a virus were to make itself known immediately—by displaying an impolite message on your screen, for example—you would immediately know that something was wrong. Additionally, if a virus immediately corrupted your machine (making it inoperable), the virus would not be able to transfer to other disks and computers. Therefore, the most common viruses are designed to replicate without users' knowledge.

When a virus does present itself, it typically is well after the point of original infection. Generally, a virus monitors for a *trigger event*, or a computer condition that causes a payload to be delivered. Trigger events include dates, time, keyboard strokes, number of file saves, number of disk accesses, file sizes, file types, and more. *Payloads*, whether designed intentionally or not, always waste productivity or harm data. Some payloads deliver “amusing” or political messages, such as the Nuclear macro virus asking for a ban on French nuclear testing. Others cause the disruption of computer processes, such as AntiCMOS preventing the user access to his or her drives. An inadvertent payload is the operation of a stealth boot virus overwriting data as it attempts to write pre-infected boot information to another part of the disk. The most lethal type of payload is inconspicuous activity and minute data damage spread across long periods of time. This is considered lethal since ultimately one may be using corrupt or irrecoverable data.

How does anti-virus software work?

Anti-virus software use a variety of counteractions to detect and remove computer viruses. Most solutions rely on three primary detection components: on-access scanning, on-demand scanning, and checksumming.

On-access scanning is similar to an automatic fire sprinkler system: A virus scan is automatically initiated on file access, such as when a disk is inserted, a file is copied, or a program is executed.

On-demand scanning is similar to a fire extinguisher: A virus scan is user initiated. On-demand scans can be performed immediately, at scheduled intervals, or at system start-up on a particular file, directory, or volume. Both on-access and on-demand scanning rely on a scanning engine, which typically utilizes a monthly updated signature file to accurately pinpoint known, generic, and even new virus signatures and characteristics.

Checksumming, also known as *integrity checking*, is a method by which an anti-virus product determines that a file has changed. Since viral code physically attaches to another file, one can determine such modification by keeping pre-infection file information. Checksumming is generally accurate and does not require any particular upgrades. Nevertheless, checksummers will not provide the virus name or type. More importantly, checksummers assume that the user has the ability to maintain a virus-free file database. Unlike scanning engines, the user must submit a virus-free file to update the checksum database registry—leaving the possibility for an infected file to be marked as valid.

Additional viral counteractions also have been added to the anti-virus arsenal. Because a virus performs an unsolicited action, such as attaching to another file without the user’s knowledge, a virus must make system calls (requesting functions through computer system’s interrupts) to operate discretely. *Interrupt monitoring* attempts to locate and prevent interrupt calls that may indicate viral action. However, a thorough monitoring of interrupts usually is obtrusive—negatively affecting system resource utilization and possibly preventing “legal” system functions. *Memory detection* depends on the recognition of a known virus’s location and code while in memory. While generally successful, this too can constrain system resources and may prevent “legal” memory use. Lastly, a new generation of virus scanning engine has been introduced under various names including *heuristics, rules-based scanning, expert systems,* or *neural nets*. These engines use a set of rules to more efficiently parse through a file and more quickly identify suspect code. While operating much faster than traditional scanners, these engines can falsely identify virus-free files.

Due to the number of virus types, effective products leverage a combination of counteraction methods. Also, the anti-virus field is constantly evolving: Involvement in virus counteraction steadily increases the knowledge base of virus research and anti-virus software vendors. This enables the refinement of detection and cure methods as well as the creation of entirely new techniques for the future.

How can I minimize my chance of infection?

McAfee’s anti-virus solutions offer a convenient and effective way to minimize the possibility of virus infection. Utilizing all the features of our anti-virus solution, including VShield—McAfee’s real-time scanning component—is imperative. While our anti-virus solutions offer automated installation, creating a virus-free system prior to installation removes even more risks. Once NetShield is installed, we suggest you scan your system regularly.

Because more than 100 new viruses are introduced each month, McAfee updates its solutions regularly. Our maintenance subscription enables you to conveniently obtain our monthly product updates to make sure your system has the most current barrier to infection.

Implementing other safe computing practices daily can further ensure virus-free operation. Scanning any new media or files introduced to your environment is the ideal way to keep computer viruses from spreading. File viruses are typically transferred from diskettes or electronically from bulletin boards or the Internet. Boot viruses are typically transferred from diskettes and are initiated by booting (starting) the computer from a boot-infected diskette. By write protecting diskettes from which you only read data, you can protect against boot and file viruses attempting to infect your diskettes. Additionally, by checking McAfee’s online forums and website, as well as the National Computer Security Association website (www.ncsa.com), you can stay up to date on the latest trends and remain virus literate.

McAfee Virus Information Library

The McAfee Virus Information LIbrary is a comprehensive database containing more than 250 technical documents and information about more than 1000 viruses. The library offers detailed information concerning computer viruses, their methods of infection, their effect on computers, instructions on removing viruses, and methods to prevent virus infection.

The McAfee Virus Information Library is available on the CD-ROM version of this software in the Windows 95 help file format. The information is also available through the McAfee Web Site.

The Virus Information Library is continuously being updated through our website to offer the most comprehensive, up-to-date information available. For more information on reaching the McAfee Web Site, see “How To Contact Us” on page 9.

E

McAfee Support Services

McAfee is pleased to offer many types of technical assistance. These flexible support programs are designed to meet the needs of individuals and businesses at any level. By offering services that range from a complimentary 90-day introductory technical support program to an optional one-year personal online maintenance and support program, McAfee ensures that all customers receive the level of support they require.

In addition, we offer a variety of technical assistance plans designed to meet the needs of business customers, including training, consulting, and enterprise support, as well as 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.

✍ *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 latest .DAT files, 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
    - McAfee BBS (electronic bulletin board system): (408) 988-4004
    - World Wide Web site: http://www.mcafee.com
    - CompuServe: GO MCAFEE
    - The Microsoft Network: 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 McAfee 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

McAfee 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
    - McAfee BBS (electronic bulletin board system): (408) 988-4004
    - World Wide Web site: http://www.mcafee.com
    - CompuServe: GO MCAFEE
    - The Microsoft Network: 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 McAfee product to the new platform (for example, from Windows 3.1 to Windows 95).

Optional support plans

✍ *Contact McAfee 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 McAfee's 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 McAfee’s Sales Support department at (408) 988-3832.

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

Professional Services Programs

McAfee 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. McAfee 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 McAfee.

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

Training

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

Consulting

McAfee 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

McAfee 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 McAfee 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

McAfee's 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 McAfee 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.

F

Reference

Scan32 Command Line Options

The following table lists all of the NetShield command options you can use when you're running Scan32 from the command line.

Example of options:

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	Scan32 automatically initiates scanning when started. Default: <depends on UI type>
/[NO]AUTOEXIT	Scan32 automatically exits if no viruses are found. If viruses are found, Scan32 does not exit (see /ALWAYSEXIT). Default: <depends on UI type>

Command-line Option	Description
/[NO]ALWAYSEXIT	Scan32 automatically exits when scan is complete. Scan32 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\NetShield\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 <server-name>	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 [<logfile>]	Enables activity logging and optionally, changes the name of the log file. Default: /LOG “NetShield Activity Log.txt”
/LOGALL	Specifies that all scan activity is logged. This option is equivalent to specifying /LOGDETECT /LOGCLEAN /LOGDELETE /LOGMOVE /LOGSETTINGS /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]LOGSETTINGS	Logs the list of configuration settings used for each scan. Default: /LOGSETTINGS
/[NO]LOGSUMMARY	Logs a summary of the completed scan. Default: /LOGSUMMARY

Command-line Option	**Description**
/[NO]LOGDATETIME	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

VSC File Format

The VSC file is a configuration text file, formatted similarly to the Windows INI file, which outlines NetShield'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, ActivityLogOptions, Scheduler, and TaskDefinitions. To edit the VSC file, right-click the filename and select Edit.

ScanOptions

Variable	Description
szProgramExtensions	Type: String Defines extensions to be used as program extensions during scan Default value: EXE COM DLL SYS DO?
szDefaultProgramExtensions -	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 subfolders 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 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

Index