# User’s Guide

## NetShield for NetWare

**McAfee, Inc.**
2805 Bowers 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

**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, send a fax to McAfee Documentation at (408) 970-9727, or send email to documentation@mcafee.com.

*Issued July 1997/ NetShield for NetWare v3.0.2*

# Table of Contents

# 1 Introducing NetShield

## Introduction

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

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

# What is NetShield?

McAfee's NetShield is a superior anti-virus solution for network servers. NetShield combines McAfee's award-winning Hunter virus scanning technology with robust server management capabilities to minimize the virus threat within networks. Hunter scanning technology achieves superior virus detection by combining several virus analysis technologies. All virus types, including Word and Excel macro, boot sector, file, multi-partite, stealth, polymorphic, and encrypted viruses are detected. The Hunter engine even stops viruses written in Visual Basic 5.0, Office 95, and Office 97 file formats, providing maximum defense against the newest threats to data security.

# Main Features

## Superior detection

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

Includes the new Hunter scanning technology that combines several types of virus analysis technologies.

Hunter technology also stops viruses written in Visual Basic 5.0 and Office97 file formats, offering users maximum defense against the newest threats to data.

Scans all virus types, including: Word and Excel macros, file infectors, multipartite, stealth, polymorphic, and encrypted viruses

## Automated protection

Automatically cleans infected files without user or administrator intervention. If the file cannot be cleaned, access to the file is automatically denied.

Scans all file accesses with minimal resource utilization.

Flexible scheduling allows administrators to configure multiple scan tasks to run at different intervals.

The Alert Manager's advanced alerting features include pager notification, e-mail notification, SNMP, event logging, and activity logging.

Centralized Alerting enables administrators to receive alerts from workstations and notify the appropriate personnel via the Alert Manager.

AutoUpdate feature allows for effortless updating of virus definition files for all servers running NetShield.

## Administrative ease

Multi-server installation capability enables administrators to simultaneously install NetShield on multiple NetWare servers.

The powerful NetShield Console makes configuring and administering NetShield servers (NetWare and Windows NT) easy.

Scan Wizard helps create new scan tasks.

NetShield's flexible Hierarchical Storage Management (HSM) support enables administrators to choose whether migrated files are scanned, thus reducing server impact and improving scanning performance.

Supports Novell Directory Services (NDS).

# How To Contact Us

## Customer service

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

McAfee, Inc.
2805 Bowers 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<br>1200 bps to 28,800 bps<br>8 bits, no parity, 1 stop bit<br>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**

139 Main Street

Unionville, Ontario

Canada L3R 2G6

Phone: (905) 479-4189

Fax: (905) 479-4540

**McAfee Europe B.V.**

Gatwickstraat 25

1043 GL Amsterdam

The Netherlands

Phone: (0) 31 20 5866100

Fax: (0) 31 20 5866101

**McAfee France S.A.**

50 rue de Londres

75008 Paris

France

Phone: 33 1 44 908737

Fax: 33 1 45 227554

**McAfee Deutschland GmbH**

Industriestrasse 1

D-82110 Germering

Germany

Phone: 49 89 89435600

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

**McAfee Japan KK**

4F Toranomon Mori Bldg. 33

3-8-12 Toranomon

Minato Ku, Tokyo, 105

Japan

Phone: 81 3 3435 8246

Fax: 81 3 3435 1349

# 2 Installing NetShield

## Before You Start

### Server requirements

To install NetShield for NetWare, you must have:

- NetWare Version 3.11, 3.12, 4.10, or 4.11
- Current minimum required NetWare patches
- At least 2MB of free disk space to install the program files

### Client requirements

- Windows 95 or Windows NT
- SPX protocol support (Microsoft or Novell)
- Client software (Microsoft Client for NetWare or Novell's Client 32)
- Microsoft NDS support (optional)
- At least 4MB of free disk space to install the program files

# Performing the Installation

| Step | Action |
|---|---|

**1.** Power up a Windows 95 or Windows NT workstation.

✍ *You must have administrator/supervisor access to the NetWare server(s).*

**2.** Do one of the following:

- If installing from CD-ROM, insert the CD-ROM.
- If installing from a file downloaded from McAfee's electronic services, decompress the zipped file into a directory on the network or your local drive.

**3.** Double-click the SETUP.EXE program in Windows Explorer or run one of the following commands from the command line:

- If installing from the CD-ROM, enter the following (replacing *x* with the drive that contains the CD-ROM):

  `x:\SETUP`

- If installing from a file downloaded from the McAfee electronic services, enter the following (replacing *x:\path* with the drive and directory where you decompressed the file):

  `x:\path\SETUP`

**Response**: The License screen is displayed. Read it carefully and click Yes.

**Response**: The Welcome screen is displayed.

**Action**: Click Next.

**Response**: The Setup Type screen is displayed.

4. Select an installation type and click Next:

   - Select Typical to install all NetShield options, including both the client and the server software.
   - Select Compact to only install the Console.
   - Select Custom to individually select installation options (e.g., Server installation only).

5. Select a folder location for the client components and click Next. To choose the default folder location, simply click Next.

   **Response**: The Select Network Servers screen is displayed.

6. Select a server and click Add. The Server Information dialog box is displayed.

   Enter an administrator name and password. Click Connect. The workstation connects to the server. Select a volume, directory location, and NDS path in which to create the NetShield NDS object. Click OK.

   ✍ *For the install software to create the NetShield NDS Object, you must have Novell Client32 installed on the client and NetWare 4.0x running on the server. If the server is running NetWare 4.0x and the NDS Path field is grayed out, you must create the NDS Object with NSHINST.NLM. For more information, see WHATSNEW.TXT.*

   Repeat this step for each server. When you are finished, click Next.

   **Response**: The Confirm Installation Settings screen is displayed.

7. Review the installation settings.

   - If the installation options are not correct, click Back and make any necessary changes.
   - If all installation options are correct, click OK. NetShield begins copying files to the server(s).

     **Response**: Once the NetShield files have been copied to the server(s), the installation program prompts you to view the WHATSNEW.TXT file.

8. To view the WHATSNEW.TXT file, click Yes.

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

To start NetShield, access the server console locally or remotely and type the following command at the server prompt:

```
netshld
```

# 3 Getting Started

## Starting the NetShield Console

To start the Console, complete the following procedure.

| Step | Action |
|---|---|
| 1. | Do one of the following:<br>▪ Click Start, point to Programs, point to McAfee NetShield, and click NetShield Console (Windows 95, Windows NT 4.x).<br>▪ From the Program Manager, open the McAfee NetShield program group and double-click the NetShield Console icon (Windows NT 3.51).<br>**Response**: The Select Computer dialog box opens. |
| 2. | Enter the name of a server or click Browse to locate one. |
| 3. | Click OK.<br>**Response**: The Login dialog box is displayed |

4. Enter the NetShield password (default: netshield) and click OK.

   ✍ *The NetShield password is completely independent of any NetWare system or user object and must be individually changed for each NetShield server. To change the NetShield password, see* *"Changing the NetShield Password" on page 21**.*

   **Response**: The Console is displayed and contains these components:

   - menu bar
   - toolbar
   - task display area

✍ *For information on using the Console, see* *Chapter 4, "Using the NetShield Console"**.*

## The menu bar

The menu bar contains the following menus and menu commands:

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

## The toolbar

The toolbar contains the following buttons:

| Tool | Description (Corresponding Menu/Command) |
|---|---|
|  | Connects to a computer (Tools/Select Computer). |
|  | Disconnects from a computer (Tools/Disconnect Computer). |
|  | Starts the Scan Wizard (Scan/Scan Wizard). |
|  | Creates a new task (Scan/New Task). |
|  | Edits a task's properties (Scan/Properties). |
|  | Copies a task (Edit/Copy). |
|  | Pastes a task (Edit/Paste). |
|  | Removes a task from the Console (Edit/Delete). |
|  | Starts the selected task (Scan/Start and Scan/Enable). |
|  | Stops the selected task (Scan/Stop and Scan/Disable). |
|  | Views the virus list (Tools/Virus List). |

### 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 33.

To edit the on-access task, see "Editing the on-access task" on page 24.

✍ *To display a task's statistics, double-click the task or highlight the task and select Statistics from the Scan menu.*

# Changing Computers

The currently connected server's name is displayed on the Console title bar. 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 is displayed (Figure 3-1).

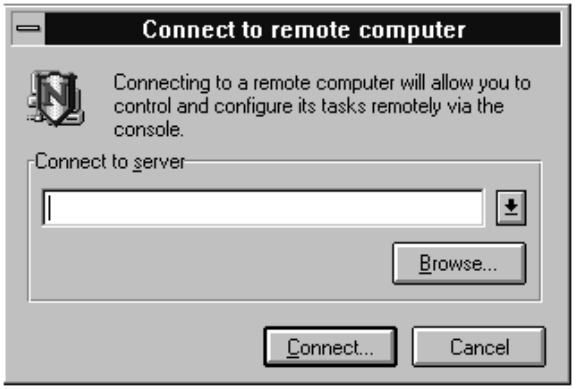



**Figure 3-1. Connect to Remote Computer Dialog Box**

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

   ✍ *The target server must have the NetShield NLM loaded.*

3. Click OK.

   **Response**: The name of the new server is displayed in the Console title bar and any configured tasks are listed in the Console task window (tasks for other servers disappear).

4. Enter the NetShield password (default: netshield) and click OK.

   ✍ *The NetShield password is completely independent of any NetWare system or user object and must be individually changed for each NetShield server. To change the NetShield password, see* *"Changing the NetShield Password" on page 21**.*

# Changing the NetShield Password

The NetShield password is completely independent of the NetWare operating system. When you first attempt to access NetShield, you must enter the following password:

```
netshield
```

To change the NetShield password, complete the following procedure:

✍ *It is recommended the administrator change the password after first installing NetShield.*

| Step | Action |
|---|---|
| 1. | Connect to a NetShield for NetWare server. |
| 2. | Select Change Password from the Tools menu. |
| 3. | Enter the old password. |
| 4. | Enter a new password. |

5. Reenter the password.

6. Click OK.

**Response**: The password is changed.

# 4 Using the NetShield Console

The NetShield Console is a component of NetShield which runs on Windows 95 workstations and Windows NT workstations and servers. The NetShield console onfigures and schedules scan tasks running on NetShield servers.

## What is a Task?

A task is a saved NetShield configuration which, once created, can be run as often as you like. Tasks can be imported and exported, copied and pasted (on-demand tasks only), and saved as configuration files. Tasks can be copied to the same server or shared between servers.

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). 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 24.

On-demand tasks are volume- and file-scanning tasks. The administrator may specify what files are scanned, how often a scan takes place, and how Net-Shield responds to infected files. For information on creating an on-demand task, see “Creating an on-demand task” on page 33.

# The On-access Task

## Editing the on-access task

The on-access task is listed in the Console task window and is preceded by a shield (  ). Although the on-access task can 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, do one of the following:

- Highlight the task and click 
- Highlight the task and select Properties from the File menu
- Right-click the task and select Properties from the shortcut menu. The NetShield property sheet is displayed with the Detection page showing.

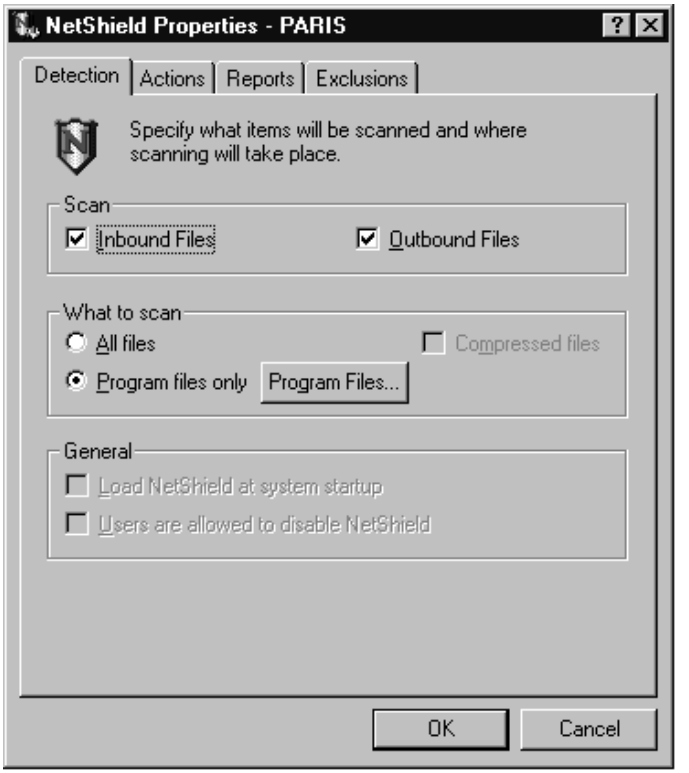



**Figure 4-1. NetShield Properties Window (Detection Property Page)**

## 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 window. |
| | **Response**: The Detection property page is displayed (Figure 4-1). |

2. Select which files to scan:

   - To scan files modified on or written to the server, select the Inbound Files checkbox.
   - To scan files read from the server, select the Outbound Files checkbox.

3. Select the types of files to scan:

   - To scan all files, select the All Files option. Skip to Step 4.
   - To scan files with specific extensions, select the Program Files Only option. Then click the Program Files button.

     **Response**: The Program File Extensions dialog box is displayed (Figure 4-2).

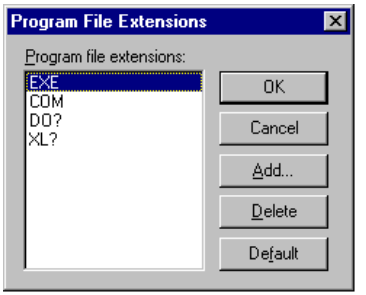



**Figure 4-2. Program File Extensions Dialog Box**

   - 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. To exit without saving, click Cancel.

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

## Setting 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 window.

   **Response**: The Actions property page is displayed (Figure 4-3).

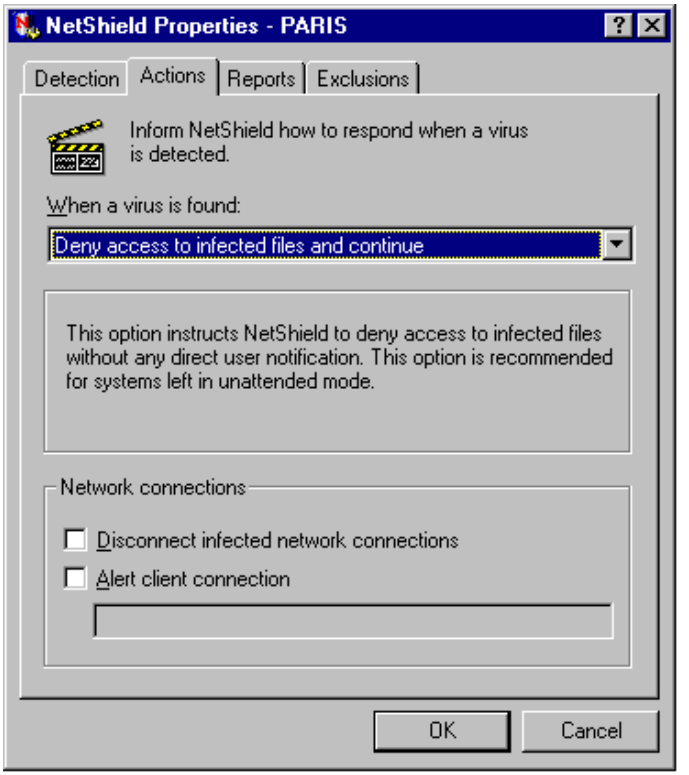



**Figure 4-3. NetShield Properties Window (Actions Property Page)**

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

   - Attempting to clean the infected files

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

   - Deleting the infected files

     If this option is selected, confirm that activity logging is enabled. This will ensure you have a record of which files were deleted, so you can restore them from backups. See “Creating a virus activity log” on page 29.

   - Denying access to the infected files

     If this option is selected, confirm that report logging is enabled. This will ensure you have a record of which files were locked, so you can clean them or restore them from backups.

   - Moving the infected files to a folder

     To help keep track of virus origination, the path to the file is duplicated in the quarantine folder. For example, if an infected file was found in SYS:DOWNLOAD\INCOMING and the quarantine directory was SYS:INFECTED the file would be moved to SYS:INFECTED\DOWNLOAD\INCOMING.

3. Select whether NetShield will disconnect infected network connections.

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

   - To configure NetShield to send a disconnect message to the infected computer, select the Alert Client Notification checkbox and enter a custom message.

     ✍ *Some operating systems, such as Windows 95 and Windows NT 4.x will automatically reconnect to the server after being disconnected. In order to prevent reconnection, the user will be denied access to the server for five minutes.*

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

## Creating a virus activity log

The virus activity 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 Window.

   **Response**: The Reports property page is displayed (Figure 4-4 on page 30).

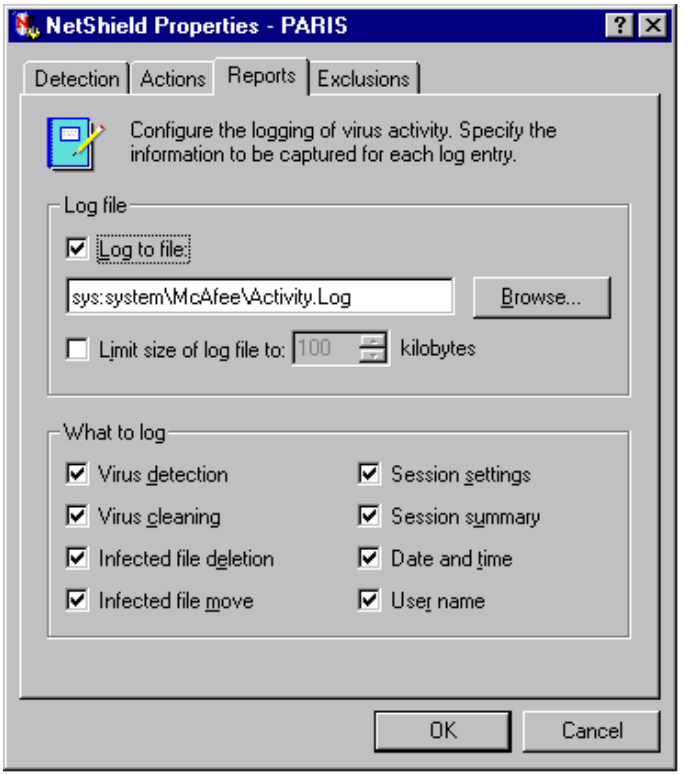



**Figure 4-4. NetShield Properties Window (Reports Property Page)**

2. Select the Log To File checkbox. To choose a new log file location and log file name, 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. Select which types of activity to include in the log file.

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

## Excluding folders from being scanned

NetShield can be configured to exclude specified files or folders from scanning.

✍ *If you configured NetShield to automatically move infected files to a folder, that 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 window.<br><br>**Response**: The Exclusions property page is displayed (Figure 4-5). |

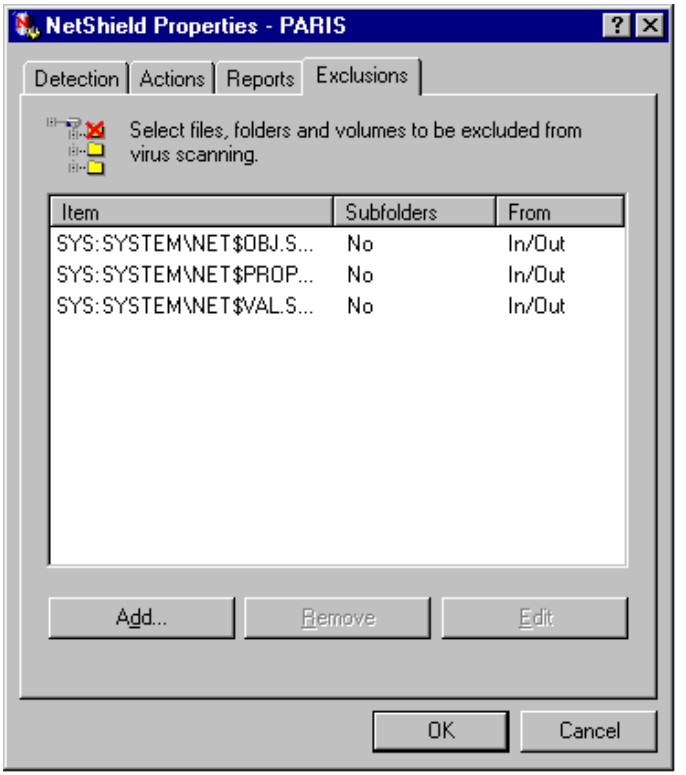



**Figure 4-5. NetShield Properties Window (Exclusions Property Page)**

2. To add an item to exclude from scanning, click Add.

   **Response**: The Exclude Item dialog box is displayed (Figure 4-6).

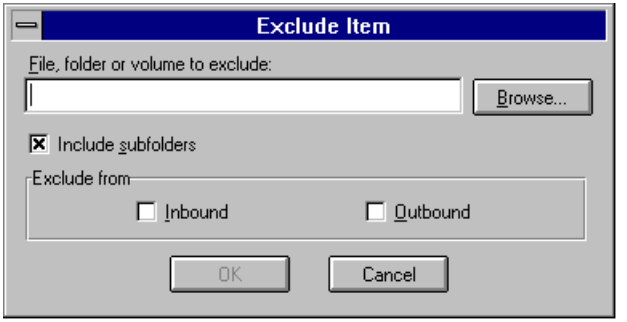



**Figure 4-6. Exclude Item Dialog Box**

3. Enter the path to the volume, folder, or file to exclude or click Browse to locate an item.

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

5. Select whether you want to exclude the item from inbound scanning (files modified on or written to the server), outbound scanning (files read from the server), or both by selecting the appropriate checkboxes.

6. Click OK.

7. Repeat steps 2 through 6 until all items to exclude 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 property 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. A new on-demand task is listed 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 properties of the on-demand task, highlight the task and click  or right-click the task and select Properties from the shortcut menu. The Task Properties window is displayed with the Detection page showing (Figure 4-7 on page 34).

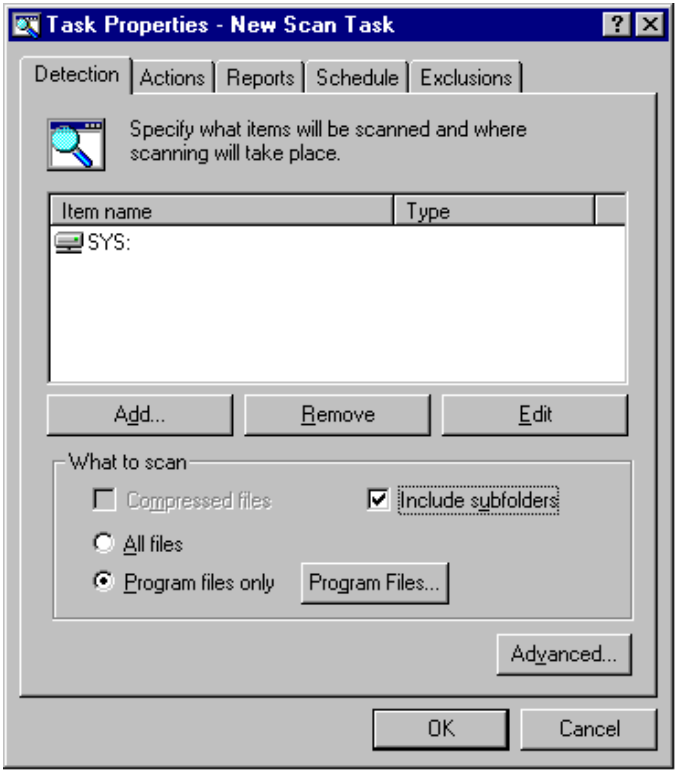



**Figure 4-7. Task Properties Window (Detection Property Page)**

## 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 Task Properties sheet.

   **Response**: The Detection page is displayed (Figure 4-7 on page 34).

2. Click Add.

   **Response**: The Add Scan Item dialog box is displayed (Figure 4-8).

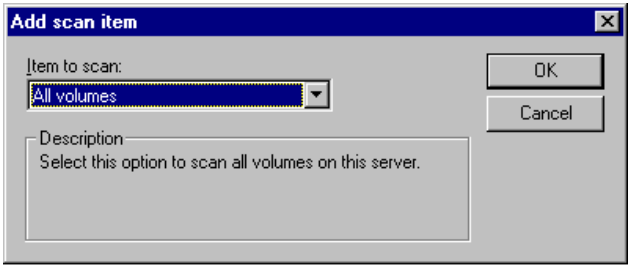



**Figure 4-8. Add Scan Item Dialog Box**

3. Select the location to scan:

   - To select an individual volume, folder, or file, select Volume, Folder or File. Click Browse, select an item to scan, and click OK.
   - To scan all volumes, select All Volumes and click OK.

4. To add more scan items, repeat steps 2 and 3.

**5.** Select the types of files to scan:

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

  **Response**: The Program File Extensions dialog box is displayed (Figure 4-9).

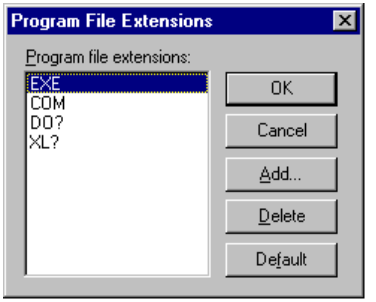



**Figure 4-9. Program File Extensions Dialog Box**

  - To add a file extension, 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 scan the item's subfolders, select the Include Subfolders checkbox.

7. 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, but impacts network perfomance less.

   - To skip scanning of mounted CD-ROMs, select the Skip CD-ROM Scanning checkbox.

   - By default, NetShield decompresses OS-compressed files, scans their contents, and recompresses them. Although this provides an extra measure of security, scanning files that are compressed by the operating system can increase the time to complete a scan. To skip scanning of OS-compressed files, select the Skip Files Compressed by the OS checkbox (NetWare 4.x and later only).

   - By default, NetShield downloads migrated files, scans their contents, and re-migrates them. Although this provides an extra measure of security, scanning files that are moved to off-line or near-line storage by Hierarchical Storage Management (HSM) systems can dramatically increase the time to complete a scan. To skip scanning of migrated files, select the Skip Migrated Files checkbox.

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

## Setting how NetShield responds to a virus infection

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

| Step | Action |
|---|---|
| 1. | Click the Actions tab of the Task Properties window. |

**Response**: The Actions property page is displayed (Figure 4-10).

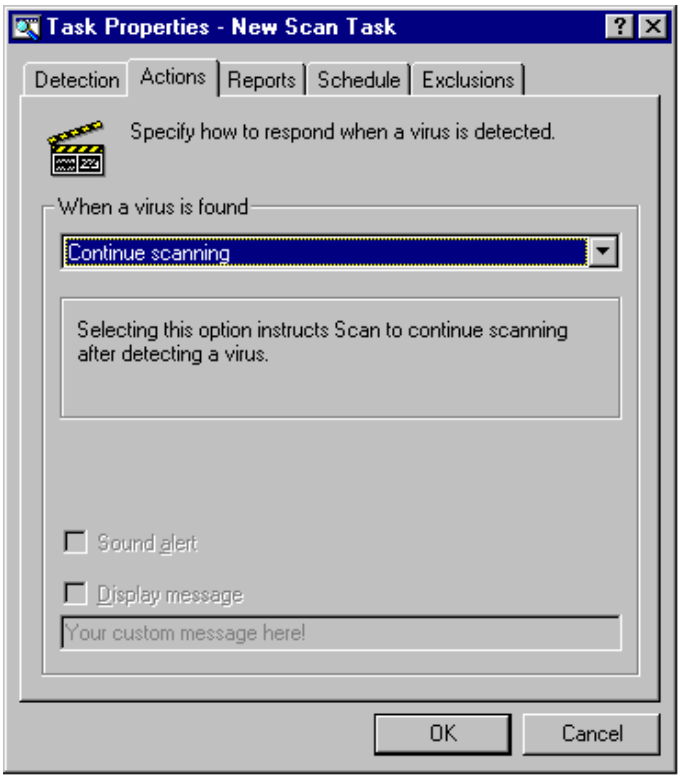



**Figure 4-10. Task Properties Window (Actions Property Page)**

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

   - Attempting to clean the infected files

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

   - Deleting the infected files

     If this option is selected, confirm that activity logging is enabled. This will ensure you have a record of which files were deleted, so you can restore them from backups. See “Creating a virus activity log” on page 44.

   - Denying access to the infected files

     If this option is selected, confirm that report logging is enabled. This will ensure you have a record of which files were locked, so you can clean them or restore them from backups.

   - Moving the infected files to a folder

     To help keep track of virus origination, the path to the file is duplicated in the quarantine folder. For example, if an infected file was found in SYS:DOWNLOAD\INCOMING and the quarantine directory was SYS:INFECTED the file would be moved to SYS:INFECTED\DOWNLOAD\INCOMING.

   - Continuing scanning

     Since no action is taken, this option is not recommended for most applications. If this option is selected, make sure to enable activity logging. This will enable you to locate which files are infected. See “Creating a virus activity log” on page 44.

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

## Scheduling an on-demand task

Decide how often to run the task:

- 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 Task Properties window.<br><br>**Response**: The Schedule property page is displayed (Figure 4-11 on page 41). |

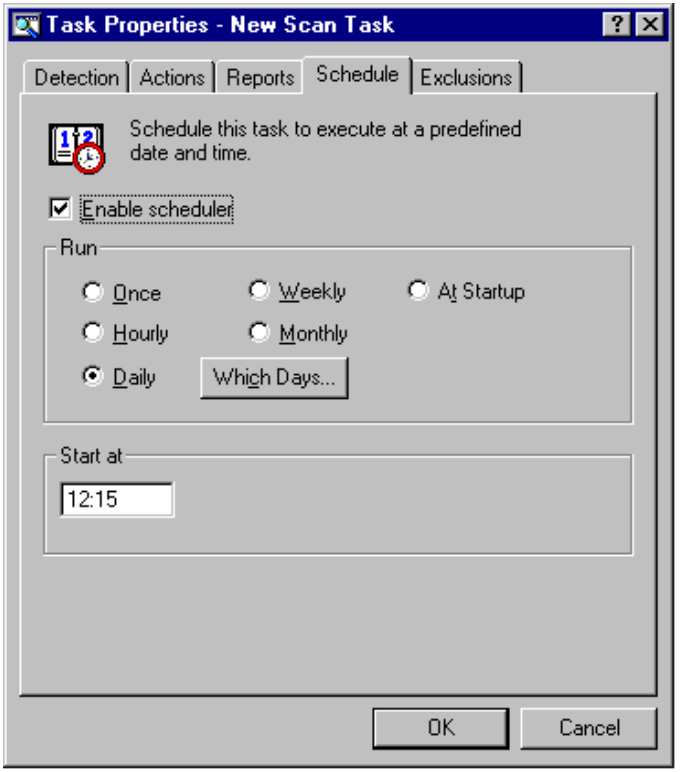



**Figure 4-11. Task Properties Window (Schedule Property Page)**

**2.** Select the Enable Scheduler checkbox.

3. Select how often the task will run:

   - To schedule a one-time scan, select the Once option and enter the time and date.
   - To schedule an hourly scan, select the Hourly option. 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.), select Hourly button and enter 30.
   - To schedule the scan for specific days, select the Daily option. Enter the time for the scan to start, and click the Which Days button.

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


**Figure 4-12. Select Days To Scan Dialog Box**

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

   - To schedule a weekly scan, select the Weekly option and enter the time and day of the week for the scan to start.
   - To schedule a monthly scan, select the Monthly option and enter the time and day of the month for the scan to start.
   - To schedule a scan every time the NetShield NLM is loaded, select the At Startup option.

4. Click OK.

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

## Creating a virus activity log

The virus activity 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 Task Properties window. |

**Response**: The Reports property page is displayed (Figure 4-13).

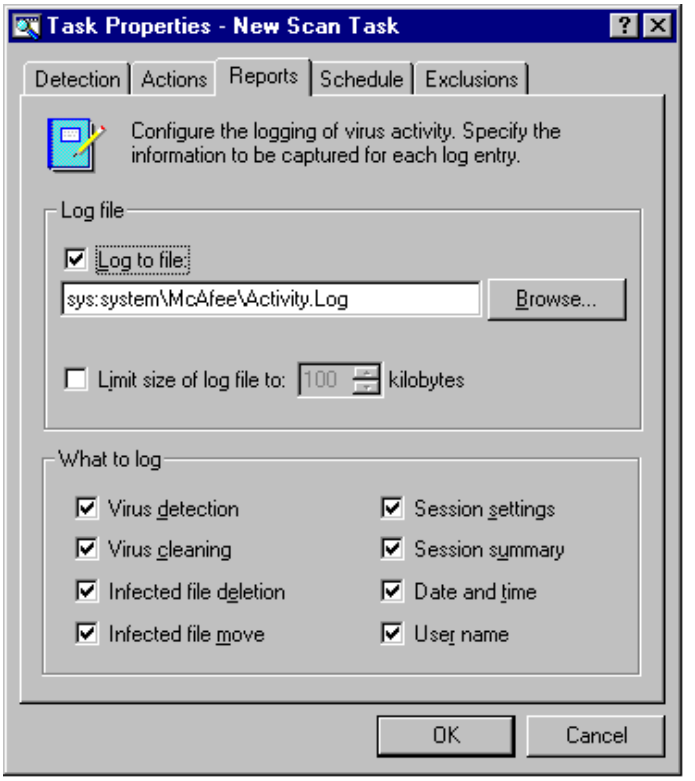



**Figure 4-13. Task Properties Window (Reports Property Page)**

2. Select the Log To File checkbox. To choose a new log file location and log file name, 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. Select which types of activity to include in the log file.

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

## Excluding folders from being scanned

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

| Step | Action |
|---|---|
| 1. | Click the Exclusions tab of the Task Properties window. |

**Response**: The Exclusions property page is displayed (Figure 4-14).

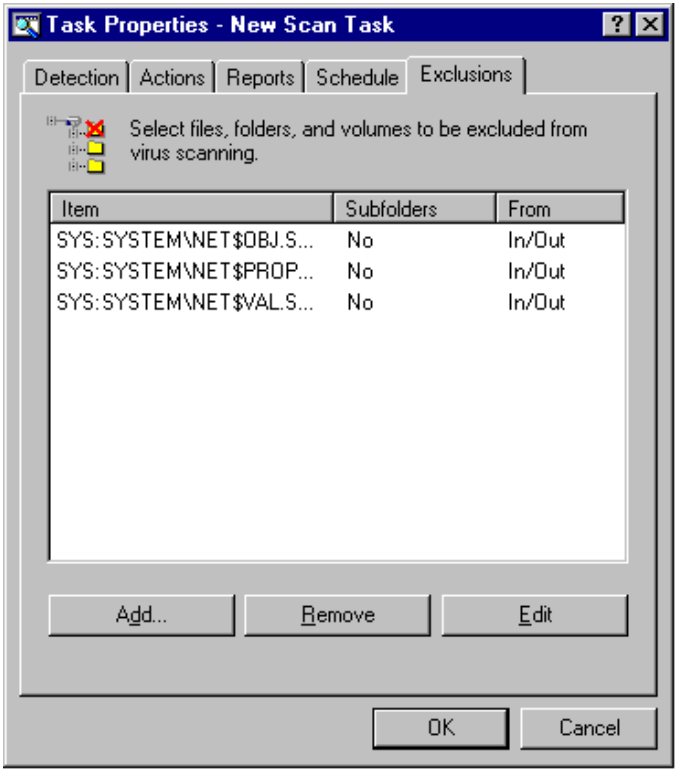



**Figure 4-14. Task Properties Window (Exclusions Property Page)**

2. To add an item to exclude from scanning, click Add.

   **Response**: The Exclude Item dialog box is displayed (Figure 4-15).

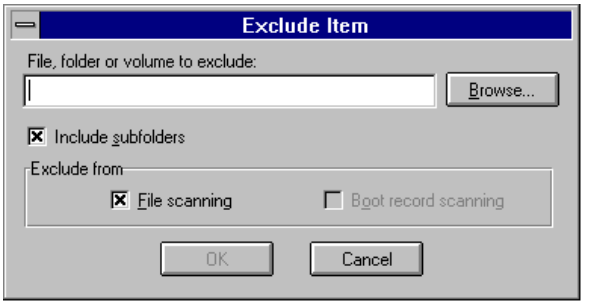



**Figure 4-15. Exclude Item Dialog Box**

3. Enter the path to the volume, folder, or file to exclude or click Browse to locate an item.

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

5. Make sure the Exclude from File Scanning checkbox is selected.

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 property 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 between servers, or import tasks from another server.

✍ *Since the formats of file system objects (e.g., scan items, log files, etc.) are not compatible between Windows NT and NetWare servers, do not copy tasks from one type of server to another. For information on the VSC file format, see "VSC File Format" on page 100.*

### 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 is displayed. |

3. Enter a path and filename or click Browse to locate one. 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 is displayed.

2. Enter the path to a VSC file or click Browse to locate one.

3. Click OK.

   **Response**: The task appears in the Console window.

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

   **Response**: The Task Properties sheet is displayed.

5. Make any necessary changes to the task and click OK.

## Copying and pasting tasks

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

✍ *Since the formats of file system objects (e.g., scan items, log files, etc.) are not compatible between Windows NT and NetWare servers, do not copy tasks from one type of server to the other.*

| 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 server, continue to the next step.
- To copy the task to another server, connect to the server. For information on connecting to another server, see "Changing Computers" on page 20.

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

**Response**: The task is copied and appears in the Console window.

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

**Response**: The Task Properties sheet is displayed.

**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, deselect the Enable Scheduler checkbox on the Schedule page. For information about using the scheduler, see “Scheduling an on-demand task” on page 40.

# 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 24.

## Deleting on-demand tasks

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

# 5 Virus Notification

In addition to automatically responding to viruses (cleaning, deleting, moving, etc.), NetShield may be configured to run a program on virus detection, receive virus activity alerts from users running VirusScan, and alert personnel of server virus activity (through pagers, printers, e-mail, etc.).

- To configure NetShield to alert personnel of virus activity through pagers, printers, e-mail, etc., see “Using AlertManager” on page 54.
- To configure NetShield to execute a program on alert, see “Executing a Program on Alert” on page 64.
- To configure NetShield to allow Centralized Alerting to report virus activity from workstations, see “Using Centralized Alerting” on page 65.
- To customize alert message text and priority levels, see “Customizing Alerts” on page 66.

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

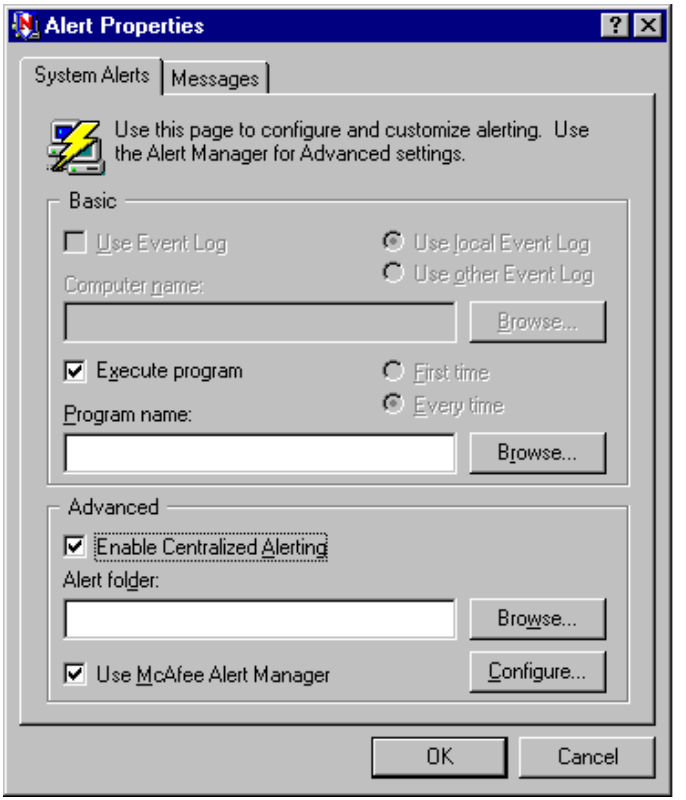



**Figure 5-1. Alert Properties Window (System Alerts Property Page)**

# Using AlertManager

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

NetShield supports the use of any combination of notification methods and multiples of each. To send additional alerts, use Forward to send alerts to another server with the NetShield NLM loaded. Whenever the server receives a Forward, 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 AlertManager, complete the following procedure:

| Step | Action |
|---|---|
| 1. | Select Alerts from the Tools menu. |
| 2. | From the System Alerts property page, select the Use McAfee AlertManager checkbox and click Configure. |

**Response**: The AlertManager Properties window is displayed with the Summary page showing (Figure 5-2).


**Figure 5-2. AlertManager Properties Window (Summary Property Page)**

## Summary page

The Summary page lists all alert notification items configured on the other property 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 server

NetShield can forward alerts to another server with the NetShield NLM loaded. The server receiving the forwarded message then sends alerts to recipients listed in the Summary page of its AlertManager property sheet.

✍ *Although NetWare servers can send Forwards to Windows NT servers, they cannot receive Forwards from Windows NT servers.*

| Step | Action |
|---|---|
| 1. | Open the AlertManager properties window. |
| 2. | Select the Forward tab.<br><br>**Response**: The Forward property page is displayed with a list of all servers configured to receive forwarded messages. |
| 3. | To add a server to receive Forwards, click Add. |
| 4. | Specify a server or click Browse to locate the server. |
| 5. | To test the Forward, click Test.<br><br>**Response**: The server receives a test message. |
| 6. | To set the priority level of the messages this server receives, click Priority Alerts.<br><br>▪ To set the server to receive low, medium, and high priority alerts, select Low.<br><br>▪ To set the server to receive medium and high priority alerts, select Medium.<br><br>▪ To set the server to receive high priority alerts only, select High.<br><br>✍ *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 server to receive forwarded alerts, click Add.

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

## Sending a network message

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

| Step | Action |
|---|---|

1. Open the AlertManager properties window.

2. Select the Network Message tab.

   **Response**: The Network Message property page is displayed with a list of all users configured to receive network messages.

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

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

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 user receives, click Priority Alerts.

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

7. Click OK.

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

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

## Sending an alert to an e-mail address

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

✍ *MHS must be running on the server sending e-mail notifications. If MHS is not running on the server, install NetShield on an MHS server, configure e-mail addresses to receive notifications on the MHS server, and configure NetShield for NetWare servers to send Forwards to the MHS server.*

| Step | Action |
|---|---|
| 1. | Open the AlertManager properties window. |
| 2. | Select the E-Mail tab.<br><br>**Response**: The E-Mail property page is displayed 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>@<workgroup> (e.g. johndoe@mcafee.com).

   Fill out the Subject line.

   Fill out the From line.

4. To configure MHS settings, click Mail Settings and enter the name of the Server and Mail Directory.

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 property page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

9. Add the following entry to the [MGMSMF] section of the MHS server's NGM.CFG file:

   ```
   sender-validation-enabled  =  FALSE
   ```

# Sending an alert to a pager

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

✍ *To send pager notifications, a modem must be installed in the NetShield server and AIO.NLM and AIOCOMX.NLM must be loaded. If the server does not have a modem, send a Forward to a modem-equipped NetShield server.*

## Alphanumeric pager

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

| Step | Action |
|---|---|
| 1. | Open the AlertManager properties window. |
| 2. | Select the Pager tab.<br><br>**Response**: The Pager property page is displayed 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 number or PIN (if applicable), and a password (if applicable). |
| 6. | To use the standard alert message, select the Use Standard Alert Message option.<br><br>To use a custom message, select the Use Custom Alert Message option and enter a message. |
| 7. | To configure the modem settings, click Modem. |
| 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 pager to receive low, medium, and high priority alerts, select Low.
   - To set the pager to receive medium and high priority alerts, select Medium.
   - To set the pager to receive high priority alerts only, select High.

10. Click OK.

11. To add another pager to receive notifications, repeat steps 3 through 10.

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

## Numeric pager

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

| Step | Action |
|---|---|

1. Open the AlertManager properties window.

2. Select the Pager tab.

   **Response**: The Pager property page is displayed 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. To configure the modem settings, click Modem.

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

11. Click OK.

12. To add another pager to receive notifications, repeat steps 3 through 11.

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

## Sending an alert to a printer

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

| Step | Action |
|---|---|

1. Open the AlertManager properties window.

2. Select the Printer tab.

   **Response**: The Printer property page is displayed 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 printer to receive low, medium, and high priority alerts, select Low.
   - To set the printer to receive medium and high priority alerts, select Medium.
   - To set the printer 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 property page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

## Using SNMP

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

| Step | Action |
|---|---|

1. Open the AlertManager property sheet.

2. Select the SNMP tab.

   **Response**: The SNMP property page is displayed.

3. Select the Enable SNMP checkbox.

4. To complete configuration of SNMP services, refer to the operating system documentation.

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

# Executing a Program on Alert

In the event AlertManager 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, you could write a batch file to send notifications to your mail package.

✍ *NetShield can launch any NCF or NLM file.*

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, select the Every Time option. To execute the program on the first alert event only, select the First Time option.

5. To save the changes and return to the console, click OK. To cancel any changes, click Cancel.

# Using Centralized Alerting

Centralized Alerting is a powerful feature for alerting the appropriate personnel of workstation virus activity. Once Centralized Alerting is enabled and configured, workstations using VirusScan report virus activity to NetShield servers. NetShield then notifies the appropriate personnel (through pagers, printers, e-mail, fax, etc.) listed in the AlertManager Summary page. To configure the AlertManager, see “Using AlertManager” on page 54.

## How Centralized Alerting works

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

✍ *For information on the Centralized Alerting file format, see “Centralized Alerting ALR File Format” on page 107.*

## Configuring Centralized Alerting

To configure Centralized Alerting, complete the following procedure:

| Step | Action |
|---|---|
| 1. | Select Alerts from the Tools menu.<br><br>**Response**: The Alert Properties window is displayed (Figure 5-3 on page 67). |
| 2. | Select Enable Centralized Alerting. |

3. Enter the location of the Alert Folder or click Browse to select one.

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

   ✍ *If VirusScan for Windows 3.1x users are using Centralized Alerting to report virus activity to this server, you should use a folder name that has eight characters or less (e.g. c:\central).*

4. Click OK.

   **Response**: NetShield is ready to receive alerts.

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

# Customizing Alerts

## Enabling/disabling alerts

To enable and disable alerts, complete the following procedure:

| Step | Action |
|---|---|
| 1. | Select Alerts from the Tools menu and click the Messages tab. |

**Response**: The Alert Properties window is displayed with the Messages page showing (Figure 5-3).

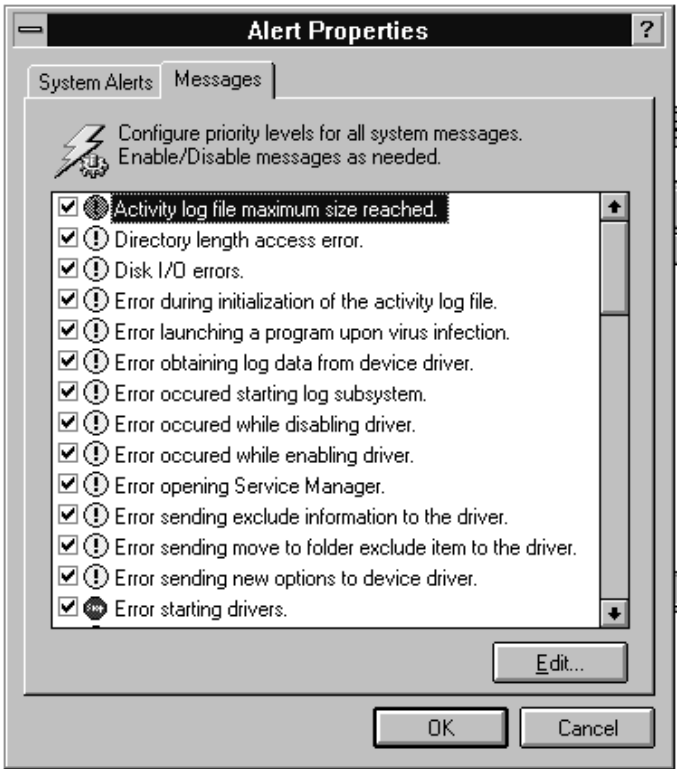



**Figure 5-3. Alert Properties Window (Messages Page)**

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 window is displayed (Figure 5-3) with the Messages page showing.

2. Highlight an alert and click Edit.

   **Response**: The Configure System Message dialog box is displayed (Figure 5-4).

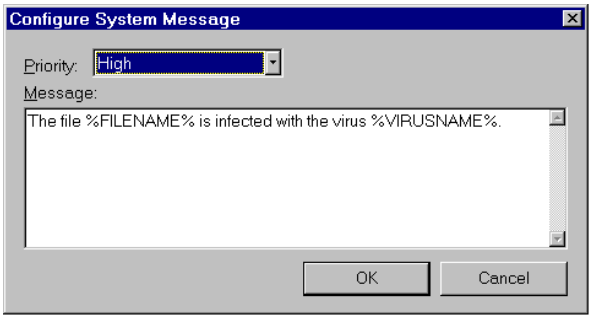



**Figure 5-4. Configure System Message Dialog Box**

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 cause of 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.<br><br>**Response**: The Alert properties window is displayed (Figure 5-3) with the Messages page showing. |
| **2.** | Highlight an alert and click Edit.<br><br>**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 the following variables:

- %FILENAME% - Name of the infected file
- %TASKNAME% - Name of the task that detected the virus
- %VIRUSNAME% - Name of the virus
- %USERNAME% - Name of the user reporting the event
- %COMPUTERNAME%- Name of the computer reporting the event
- %SOFTWARENAME% - Software product reporting the event
- %SOFTWAREVERSION% - Version of the software reporting the event
- %DATE% - Date of the event
- %TIME% - Time of the event

# 6 Updating NetShield

## Overview: AutoUpdate

Approximately once a month, McAfee updates the NetShield data (DAT) files. To distribute these files, a multi-line bulletin board system, a forum on CompuServe, and an Internet node are available. For more information on obtaining DAT files, see “Updating Virus Definition Files” on page 82.

AutoUpdate is a powerful feature that can ensure you always have the latest version of the anti-virus data files on your systems. Once AutoUpdate is properly configured, you can simply update a single server and all servers running NetShield for NetWare will be updated with the most current version of the NetShield DAT files.

Servers can be configured to provide or accept updates. A server scheduled to accept updates broadcasts a DAT file version request to other servers running NetShield for NetWare. Any servers configured to provide updates send version information to the requesting server. The requesting server then evaluates the received information and chooses the server with the most current DAT files. If more than one server has the same DAT file version, the server which responded first is chosen.

After the new DAT files are received, they are copied over the old DAT files. NetShield must then be reinitialized. Depending on how the server is configured, reinitialization occurs automatically or may need to be done from the server console.

# Updating Strategies

When configuring AutoUpdate, it is important to meet the needs of your environment. This typically involves using the trusted source strategy, the rumor strategy, or a combination of both.

## Trusted source strategy

Using the trusted source strategy, each server is configured to only accept data file updates from a trusted server. Simply update the master server and each server checks in for the “official news” (Figure 6-1).

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

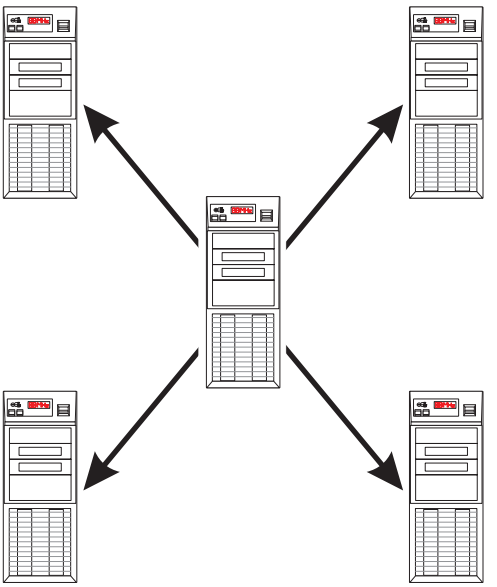


**Figure 6-1. Command-and-Control Strategy**

## Rumor strategy

Using the rumor strategy, all NetWare servers are configured to provide and accept data file updates. Whenever any NetWare server is updated, the updated DAT files are passed around like a rumor, and all servers configured to accept updates eventually “get the news” (Figure 6-2).

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

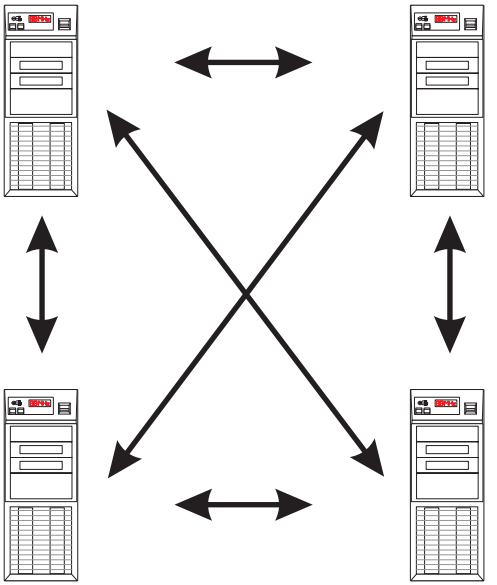


**Figure 6-2. Rumor Strategy**

# Configuring AutoUpdate

To configure AutoUpdate, complete the following procedure:

| Step | Action |
|---|---|

1. Select AutoUpdate from the Tools menu.

   **Response**: The AutoUpdate Properties window is displayed with the Update Method property page showing (Figure 6-3).

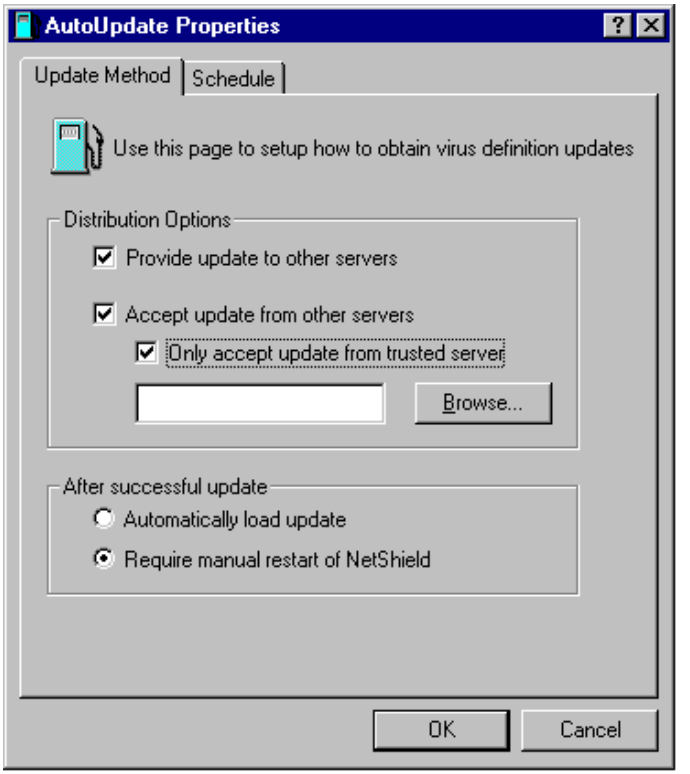



**Figure 6-3. AutoUpdate Properties Window (Update Method Property Page)**

2. To configure this server to provide updates to other servers, select Provide Updates to Other Servers.

3. To accept updates from other servers, select Accept Updates from Other Servers.

4. To configure this server to only accept updates from a trusted server, select Only Accept Updates from Trusted Server. Enter the name of the trusted server or click Browse to locate a server.

5. Select from the following:

   - To configure NetShield to automatically load the update, select Automatically Load Update.

   - To manually reinitialize NetShield at the server console, select Require Manual Restart of NetShield.

6. Select from the following:

   - If this server accepts updates, you must schedule when the server makes requests for updates. See “Scheduling AutoUpdate” on page 76.

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

# Scheduling AutoUpdate

For a server to receive updates, it must be scheduled to request them. AutoUpdate can request updates:

- Once
- Hourly
- Daily
- Weekly
- Monthly
- At Startup

To schedule AutoUpdate, complete the following procedure:

| Step | Action |
|---|---|
| 1. | Click the Schedule tab of the AutoUpdate Properties window. |

**Response**: The Schedule property page is displayed (Figure 6-4).

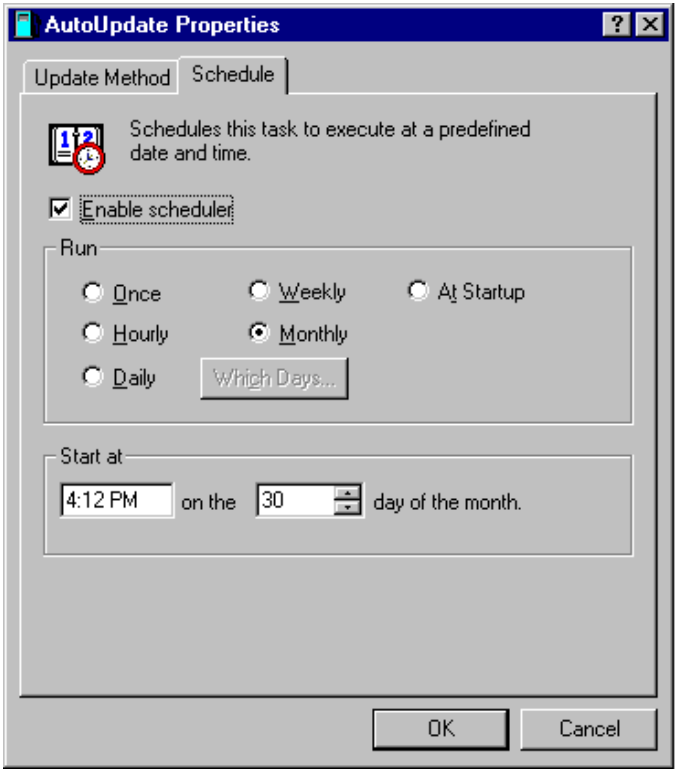



**Figure 6-4. AutoUpdate Properties Window (Schedule Property Page)**

2. Select the Enable Scheduler checkbox.

**3.** Select how often the server requests updates:

- To schedule NetShield to request a one time update, select the Once option and enter the time and date.
- To schedule NetShield to request an update hourly, select the Hourly option. Set the request to start x minutes after the hour where x is a number between 0 and 59. For example, to set the request to occur 30 minutes after every hour (8:30, 9:30, 10:30, etc.), select the Hourly option and enter 30 in the minutes field.
- To schedule NetShield to request an update weekly, select the Weekly option and enter the time and day of the week for the request to start.
- To schedule NetShield to request an update monthly, select the Monthly option and enter the time and day of the month for the request to start.
- To schedule NetShield to request an update at Startup, select the At Startup button.
- To schedule NetShield to request an update on specific days, select the Daily option and enter the time for the request to start. Then, click the Which Days button.

  **Response**: The Select Days to Request Updates dialog box is displayed (Figure 6-5).


**Figure 6-5. Select Days To Request Updates Dialog Box**

**Action**: Choose which days the update request will run. Click OK.

4. Click OK.

**Response**: AutoUpdate is scheduled to run at the specified time(s).

# A Encountering Viruses

## Removing Viruses

When NetShield detects a virus in a file, it will take the action specified during configuration. See “Setting how NetShield responds to a virus infection” on page 27 (on-access scanning) or “Setting how NetShield responds to a virus infection” on page 38 (on-demand scanning).

### If you selected Clean Infected Files

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

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

### If you selected Delete Infected Files

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

If this option is selected, confirm that report logging is enabled. This will ensure you have a record of which files were deleted, so you can restore them from backups. See “Creating a virus activity log” on page 29 (on-access scanning) and “Creating a virus activity log” on page 44 (on-demand scanning).

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

## If you selected Move Infected Files

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

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

## If you selected Continue Scanning

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

✍ *This option is not recommended for most applications. If you do use this option, make sure report logging is enabled. See "Creating a virus activity log" on page 29 for on-access scanning or "Creating a virus activity log" on page 44 for on-demand scanning.*

# B Updating Virus Definition 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 200 new viruses. To find out what's new, read the WHATSNEW.TXT text file that shipped with this product.

## Download new versions

Download the latest virus definition data (DAT) files from the McAfee website, www.mcafee.com, or from another of McAfee's online services. For more information, see "How To Contact Us" on page 9.

To update your DAT files, 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. |

✍ *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 NetShield program directory. The default directory location is shown below.

✍ *MCALYZE.DAT is not required by NetShield for NetWare.*

SYS:MCAFEE\NETSHLD

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

## 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

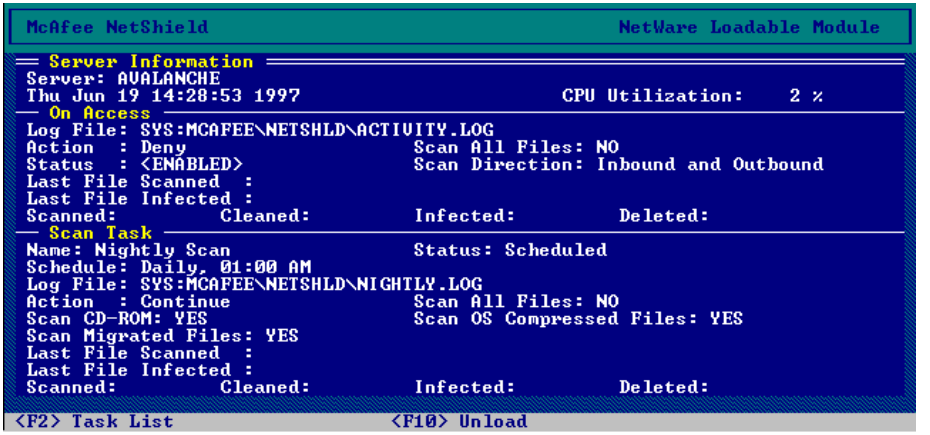
# NetShield Server

The NetShield NLM has a limited user interface which contains information on the on-access task and scan tasks.

To load the NetShield NLM, type the following command at the server prompt:

```
netshld
```

> **Response**: The NetShield NLM server screen is displayed. It contains information on the on-access task and the currently selected scan task.



To display the properties of another scan task, press F2.

**Response**: The task list is displayed.

**Action**: Select another task and press ENTER.

**Response**: The NetShield server screen opens with the task's properties displayed.

To unload the NetShield NLM, press F10.

# 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 200 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.
- More than 70% of infections occur through diskette distribution.
- More than 80% of infections result in lost productivity, and 35% result in lost data.
- More than 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.
- More than 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 widespread virus is a new type called a *macro virus*. Macro viruses use an application's macro language to spread to other documents within that application and perform unsolicited actions. Word macro viruses ae 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 200 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 through the McAfee Web Site.

The Virus Information Library is continuously being updated 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 different types of technical assistance to customers. These flexible support programs are designed to meet the needs of individuals and businesses at any level. By offering support solutions that range from a complimentary 90-day introductory technical support program to an optional one-year personal support plan, McAfee helps to ensure that you receive the level of technical assistance you require.

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

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

# Customer Service Programs

## Free introductory support program

All registered owners of single-node (one computer) products, such as those purchased at local retail stores or those downloaded from McAfee Store on our website, are entitled to:

- Free online virus signature (.DAT) file updates for the life of the product.
- One year of free online product upgrades (product version revision) with the newest features with a VirusScan Classic purchase; two years of free online product product upgrades with a VirusScan Deluxe purchase.
- Free support services listed below

### Support services

- 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
  - Microsoft Network: MCAFEE
  - America Online: keyword MCAFEE
- Technical support phone assistance, available during regular business hours, 6:00 A.M.– 6:00 P.M. Pacific time, Monday through Friday, for 90 days. To receive support, contact our professionally-trained support representatives at one of the following numbers:
  - For corporate-licensed customers: (408) 988-3832
  - For retail-licensed customers: (972) 278-6100

To receive your free online upgrades, please refer to the download instructions included in the box or contact our Customer Care 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.

## Free subscription maintenance and support program

McAfee offers all registered owners of licensed multiple-node (ten computers or more) subscription products the following free support services and maintenance during the two-year term of the software subscription.

✍ *You must be registered to receive these services.*

### Support services

- 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 definition data. If you upgrade your operating system, you can also extend the upgrade of your McAfee product to the new platform.

# Optional support plans

✍ *Contact McAfee for current pricing structures.*

## Option 1: One-year personal support plan

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 protection 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-ROM 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 CD-ROMs (depending on the product) and a quarterly update newsletter. With this option, you can update your product to include the latest features and virus data files without having to download 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 Customer Care 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.

## Training

McAfee's expertise and experience is available to your personnel, allowing an organization to take full advantage of its 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
- Installing and configuring McAfee products
- Configuring Windows 95
- 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 corporate 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)

Every 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 7 x 24 enterprise 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.

✍ *McAfee reserves the right to change part or all of its Professional Services Programs at any time without notice.*

# F

# Reference

## VSC File Format

The VSC file is a configuration text file, formatted similarly to the Windows INI file, which outline NetShield task definitions. 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 three groups: ScanOption, AlertOptions, and ActivityLogOptions. To edit the VSC file, right-click the filename and select Edit.

### ScanOptions

| Variable | Description |
|---|---|
| szProgramExtensions | Type: String<br>Defines extensions to be used as program extensions during scan<br>Default value: EXE COM DLL SYS DO? |
| szDefaultProgramExtensions - | Type: String<br>Defines extensions to be used as default program extensions during scan configuration<br>Default value: EXE COM DLL SYS DO? |

| Variable | Description |
|---|---|
| bIncludeSubFolders | Type: Boolean (1/0)<br>Instructs scanner to search for viruses inside sub-folders<br>Default value: 1 |
| bScanAllFiles | Type: Boolean (1/0)<br>Instructs program to scan inside all files<br>Default value: 0 |
| bScanCompressed | Type: Boolean (1/0)<br>Instructs program to scan inside compressed files (PkLite, LZEXE, ZIP)<br>Default value: 1 |
| uScanAction | Type: Integer (1-5)<br>Defines what action will be taken upon virus detection:<br>1 - Prompt for Action<br>2 - Continue Scanning<br>3 - Move Infected File<br>4 - Clean Infected File<br>5 - Delete Infected File<br>Default value: 1 |
| bAutoStart | Type: Boolean (1/0)<br>Defines if scan will be started immediately upon launch<br>Default value: 0 |
| bAutoExit | Type: Boolean (1/0)<br>Defines if scanner will be unloaded when scan is finished<br>Default value: 0 |

| Variable | Description |
|---|---|
| nPriority=0 | Type: Integer (0-5)<br>Defines the priority at which scan is to be executed<br>Default value: 3 |
| szScanItem=C:\ | Type: String<br>Defines item to be scanned<br>Default value: C:\ |

## AlertOptions

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

## ActivityLogOptions

| Variable | Description |
|---|---|
| bLogToFile | Type: Boolean (1/0)<br>Defines if scan results should be logged into log file<br>Default value: 1 |
| bLimitSize | Type: Boolean (1/0)<br>Defines if size of the log file should be limited<br>Default value: 1 |
| uMaxKilobytes | Type: Integer<br>Defines maximum size of the log file<br>Default value: 100 |

| Variable | Description |
|---|---|
| szLogFileName | Type: String<br>Defines log file name<br>Default value: NetShield Activity Log.txt |
| bLogDetection | Type: Boolean (1/0)<br>Defines if scan results should be logged<br>Default value: 1 |
| bLogClean | Type: Boolean (1/0)<br>Defines if clean results should be logged<br>Default value: 1 |
| bLogDelete | Type: Boolean (1/0)<br>Defines if infected file delete operations should be logged<br>Default value: 1 |
| bLogMove | Type: Boolean (1/0)<br>Defines if infected file move operations should be logged<br>Default value: 1 |
| bLogSettings | Type: Boolean (1/0)<br>Defines if session settings should be logged<br>Default value: 1 |
| bLogSummary | Type: Boolean (1/0)<br>Defines if session summary should be logged<br>Default value: 1 |
| bLogDateTime | Type: Boolean (1/0)<br>Defines if time and date of an event should be logged<br>Default value: 1 |

| Variable | Description |
|---|---|
| bLogUserName | Type: Boolean (1/0)<br>Defines if user name should be logged<br>Default value: 1 |

## Scheduler

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

## TaskDefinition

| Variable | Description |
|---|---|

| | |
|---|---|
| szTaskName | Type: String<br>Defines task name<br>Default value: New Scan Task |
| wTaskAttrib | Type: Integer<br>Contains task attributes<br>Do not modify |
| wTaskType | Type: Integer<br>Contains task type<br>Do not modify |

# Centralized Alerting ALR File Format

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

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

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

# Index