Using NetShield

Version 2.1

Contents

Chapter 1 Welcome to NetShield

Chapter 2 Installation and Setup

Chapter 3 Using NetShield

Index

Chapter 1 Welcome to NetShield

Thank you for purchasing McAfee Inc.'s NetShield™ software, a powerful and advanced system designed to detect computer viruses on a NetWare server. NetShield monitors server input and output, and protects against virus infections from workstations, bridges, and modems.

NetShield is a NetWare Loadable Module (NLM). This allows it to integrate easily into your NetWare environment and function independently of any workstation, guaranteeing that your network is always protected.

NetShield tasks

It is important that you install and configure NetShield correctly for your particular network. As you set up NetShield, you'll complete the tasks necessary to maintain a virus-free network. Use this task list as a roadmap for applying the information in this reference to your network.

- **Task 1: Installation.** You'll install NetShield on every server at your site. Download the NetShield files and copy them to the SYS:SYSTEM directory on your server. For NetWare 3.11 or 3.12 installations, you also need to download and install Novell patches. Refer to Chapter 2, "Installation and Setup," for details.

  Note: If you use a bootable floppy diskette to start your server, make sure that the boot diskette is clean of any viruses. The documentation for VirusScan™, a McAfee virus scanning product that can be used on a workstation, describes a procedure for creating a clean bootable diskette.

- **Task 2: Configuration.** Set NetShield to run scans at regular intervals, using the "periodic" scanning settings. Turn on Cyclic Redundancy Checking (CRC) if you have a stable file environment. CRC checking verifies that numeric check sums stay consistent for files. If files are changed often, then an error in the check sums will be reported. Finally, set NetShield to scan all files transferred to the server, using the "on-access" scanning settings. Refer to "Configuration Recommendations" in Chapter 3, "Using NetShield," for details.
- **Task 3: Scanning.** Once you've configured NetShield, it will automatically scan in the background. The NetShield NLM will be running as long as your NetWare server is running.

- **Task 4: Reporting.** NetShield can inform you when a virus is found, both by broadcasting a network message to selected users and by recording the information in a log file. It can then move or delete the infected file. We recommend that you set up NetShield to log infections in a file, notify the network supervisor, and move infected files into a "quarantine" directory for later inspection. Refer to "Configuring Virus Reporting" in Chapter 3, "Using NetShield," for details.
- **Task 5: Updating.** As new viruses are found, McAfee will release new virus signature files for you to install. When you receive an update, or download one from the McAfee BBS, update one server and enable cross-server updating so that the new list is copied to the other servers over the network.
- **Task 6: Virus elimination.** Once you've identified and isolated an infected file, eliminate the virus using other McAfee products such as VirusScan and VShield™. Scan does periodic scanning of a single PC and removes viruses from a single PC, while VShield does on-access scanning of a single PC.

System requirements

The NetShield program requires a Novell NetWare 386 v3.11, 3.12, or 4.1 file server with at least 718Kb of free server RAM. It should utilize no more than 10% of server CPU time. Additional patches are needed for NetWare 3.11 or 3.12 installations (refer to Chapter 2, "Installation and Setup," for details.)

NetShield is not compatible with version 3.10 of Novell NetWare 386.

How to use this manual

This manual will help you get NetShield running quickly and properly.

- Chapter 1, "Welcome to NetShield," describes the NetShield program, general tasks for using NetShield, and system requirements.
- Chapter 2, "Installation and Setup," describes how to install, load, and maintain your NetShield software.
- Chapter 3, "Using NetShield," contains reference information laid out in a format that matches the NetShield menus. If you need help navigating the menus, look for the guides at the start of each of these chapters.

How to contact McAfee

To contact McAfee for sales and product support:

Phone	(408) 988-3832 Monday through Friday 6:00 am to 5:00 pm Pacific Standard Time
Fax	(408) 970-9727
Online 24-hour access (refer to "Online Access" later in this section)	McAfee BBS CompuServe Internet

Before you call

For fast and accurate help, please have the following information ready when you contact McAfee:

- Program name and version number.
- Type and brand of computer, hard disk, and any peripherals.
- Version of DOS you are using.
- Version of NetWare you are using.
- Printouts of your AUTOEXEC.NCF and STARTUP.NCF files.
- A description of the exact problem you are having. Please be as specific as possible. If you can't be at your computer when you call, a printout of the screen will be helpful.

If you are overseas, you can contact a McAfee authorized agent. Agents are located in more than 50 countries around the world and provide local sales and support for our software.

On-line access to updates and technical support

McAfee updates its software approximately monthly to add new virus detectors, new options, and fix reported bugs. To distribute these new versions, we run a multi-line bulletin board system, a forum on CompuServe, and an Internet node.

McAfee bulletin board system (BBS)

Our multiline BBS is accessible 24 hours a day, 365 days a year, except for scheduled downtime and maintenance. All lines run high-performance modems operating from 1,200 bps to 28,800 bps with line settings of 8 data bits, no parity, and 1 stop bit. Both technical support and software updates are available on the bulletin board. The McAfee BBS phone number is (408) 988-4004.

McAfee Forum on CompuServe

We sponsor the McAfee Virus Help Forum on CompuServe. To reach it, type **GO MCAFEE** at any CompuServe prompt.

Internet access

The latest versions of McAfee's anti-virus software are available by anonymous ftp (file transfer protocol) over the Internet from the site **ftp.mcafee.com**. If your domain resolver does not support names, use the IP address 192.187.128.3. Enter **anonymous** or **ftp** as your user ID and your own e-mail address as the password. Programs are located in the pub/antivirus directory. If you have questions, please send e-mail to **support@mcafee.com**.

You can also find McAfee's anti-virus software at the SimTel Software Repository at **Oak.Oakland.EDU** in the **simtel/msdos/virus** directory and its associated mirror sites:

wuarchive.wustl.edu (US)

ftp.switch.ch (Switzerland)

ftp.funet.fi (Finland)

src.doc.ic.ac (UK)

archie.au (Australia)

Other sources of information

The McAfee BBS and CompuServe Virus Help Forum are excellent sources of information on virus protection. Batch files and utilities to help you use VirusScan software are often available, along with helpful advice.

Independent publishers, colleges, training centers, and vendors also offer information and training about virus protection and computer security.

We especially recommend the following books:

- Ferbrache, David. *A Pathology of Computer Viruses*. London: Springer-Verlag, 1992. (ISBN 0-387-19610-2)
- Hoffman, Lance J. *Rogue Programs: Viruses, Worms, and Trojan Horses*. Van Nostrand Reinhold, 1990. (ISBN 0-442-00454-0)
- Jacobson, Robert V. *The PC Virus Control Handbook*, 2nd Ed. San Francisco: Miller Freeman Publications, 1990. (ISBN 0-87930-194-0)
- Jacobson, Robert V. *Using McAfee Associates Software for Safe Computing*. New York: International Security Technology, 1992. (ISBN 0-9627374-1-0)

In addition, the following sources can provide useful information about viruses:

- National Computer Security Association (NCSA), 10 South Courthouse Avenue, Carlisle, PA 17013
- CompuServe VIRUSFORUM
- Internet **`comp.virus`** newsgroup

Chapter 2 Installation and Setup

Installing NetShield is a straightforward process. You simply download the NetShield 2.1 files, copy them to the SYS:SYSTEM directory on your server, modify the AUTOEXEC.NCF file to load NetShield automatically upon server startup, then load NetShield. If you are running Novell v3.11 or 3.12, you also need to install NetWare patches obtained from Novell or McAfee. This chapter describes these tasks in detail.

Note: If you are upgrading from an earlier version of NetShield, be sure to back up the files in your NetShield directory before proceeding.

Step 1: Download the NetShield software

Obtain the latest NetShield software from the McAfee BBS, CompuServe, or the Internet. Refer to "Contacting McAfee" in Chapter 1, "Welcome to NetShield," for information about accessing these services.

Downloading files

Download and uncompress the latest NetShield compressed (.ZIP) files. It contains the following files:

Filename	Description
NETSHLD.NLM	NetShield 2.1 NLM file
NAMES.DAT	Virus Scanner data file
SCAN.DAT	Virus Scanner data file
VIR$CFG.DAT	NetShield 2.1 base configuration file
NETSHLD2.TXT	NetShield 2.1 documentation

Copying files

Copy these files to the SYS:SYSTEM directory on your NetWare server. You can choose a different location on your server, but we recommend this directory. If you choose a different directory, you need to add that directory to the search path using the NetWare SEARCHADD command. For more information, see your Novell documentation.

Unless otherwise specified, NetShield creates, loads, and saves configuration files, log files, and reports in the directory where the NETSHLD.NLM file is located.

Note: You must be logged in with create and delete rights to the directory on the target server volume.

Validating NETSHLD.NLM

When you download a program file from any source other than the McAfee bulletin board or other McAfee service, it is important to verify that it is authentic, unaltered, and uninfected. McAfee anti-virus software includes a program called Validate that helps you do this. When you receive a new version of VirusScan, run Validate on all of the program files.

To do this for VirusScan, start from the system prompt (C> or [C:\]):

1. Change to the directory to which you have downloaded the files. For example, if you have stored the files in C:\MCAFEE\DOWNLD:

   ```
   C> c:
   C> cd \mcafee\downld
   ```

2. Type the command:

   ```
   C> validate netshld.nlm
   ```

3. Compare the results with the information in the README.1ST file or other text file for the program you validated. If the validation results match what is in the file, it is highly unlikely that the program has been modified.

Step 2: Download NetWare Patches (NetWare 3.11 or 3.12 sites only)

NetShield requires some NetWare patch files for NetWare 3.11 and 3.12. Use the following recommended versions (in parentheses) or higher:

A3112.NLM (4.10A)	AFTER311.NLM (4.10A)	CLIB.NLM (3.12h)
MATHLIB.NLM (3.12h)	MATHLIBC.NLM (3.11h)	NWSNUT.NLM (4.11)

Novell supplies these patches in the LIBUP4.EXE file. To obtain this file

- From Novell, see the Novell NetWire on CompuServe, the ftp.novell.com anonymous ftp site on the Internet, or other Novell on-line services.
- From McAfee, download it from the McAfee BBS under File Area "P" (for Patches), or from the mcafee.com FTP site in the pub/patches directory.

Copy these files to the SYS:SYSTEM directory on your NetWare 3.11 or 3.12 server.

Note: *Do not* install these patches on a NetWare 4.x server.

Step 3: Customizing the AUTOEXEC.NCF File

We recommend that you change your server's AUTOEXEC.NCF file so that NetShield loads automatically whenever the server starts up.

To edit this file, use the NetWare LOAD INSTALL command (for more information, refer to your Novell documentation). Add the following command line to this file:

LOAD NETSHLD DEFAULT

For a description NetShield load options, refer to the next section, "Loading NetShield."

Save your changes, then restart your server for these changes to take effect.

Step 4: Loading NetShield

Now that you have installed NetShield, you can load it using various stored settings. You can use the default NetShield settings, the settings stored in the standard configuration file (VIR$CFG.DAT), or those stored in a custom configuration file. NetShield creates VIR$CFG.DAT automatically when you load the program for the first time.

Load NetShield using one of the following options:

- To run NetShield with the default settings and no configuration file, use this command:

  ```
  LOAD NETSHLD
  ```

- To run NetShield with the default configuration file, VIR$CFG.DAT, from the SYS:SYSTEM directory, use this command:

  ```
  LOAD NETSHLD DEFAULT
  ```

- To run NetShield with a user-specified configuration file from the directory you specify, use the following command:

  ```
  LOAD NETSHLD [path \ filename]
  ```

  If the configuration file does not reside in the same directory as NetShield, you must specify the complete path, including the volume name. You can enter these commands at the NetWare server console prompt or the remote login prompt. Alternatively, you can have them execute automatically in the AUTOEXEC.NCF file.

Note: *Do not* load NetShield 2.1 with a version 1.x configuration file. NetShield Version 1.x configuration files are not compatible with NetShield Version 2.1.

Step 5: Viewing NetShield's Opening Screen

When you first load NetShield, a screen similar to the following example is displayed:

```
 NetShield Version 2.1             NetWare Loadable Module
 McAfee, Inc. NetShield Virus Protection For File Server
                         SERVER1
                     Mon Feb 20, 1995

                    NetShield Main Menu Options

                    Immediate Scan
                    Configure Scanning Mode
                    Configure Virus Detection
                    Configure NetShield NLM
                    Configure Virus Reporting
                    Configure Network Security

 Press F10 To View Scanning Statistics
```

The **Main menu** is the highest-level menu in the hierarchy. The NetShield menu system uses conventional NetWare keys for menu navigation. You highlight, select, and exit menus as you would any NetWare utility, such as SYSCON. For general instructions about navigating NetWare menus, refer to your Novell documentation.

You can press F10 at any time to display the **Status window**, which shows the current status of many of the NetShield configuration settings. The following example shows the initial NetShield default settings.

```
NetShield Version 2.1              NetWare Loadable Module

Volume Scanning:     DISABLED   NetShield Delay Factor:  3
On Access Scanning:  DISABLED   CPU Utilization:   0 percent
Periodic Scanning:   DISABLED   Detection Action: Ignore
Logging:             DISABLED
CRC Checking:        DISABLED   Mon Sep 19 15:01:45 1994
User Alarms:         DISABLED
Console Messages:    DISABLED
Network Monitoring:  DISABLED   Access Time Remaining 0 Minutes

Volume Scanning Statistics
 Scanning:
 Detected:
Periodic Scanning Statistics
 Scanning:
 Detected:
On Access Scanning Statistics
 Inbound:
 Detected:
 Outbound:
```

```
    Detected:

Press F10 To View Menus
```

Press F10 again to return to the current menu. Most scanning options are disabled or configured to minimum settings. For more information about the features listed in NetShield's Status window, refer to Chapter 3, "Using NetShield."

Exiting NetShield

You can unload NetShield from server memory to free up server resources. Exiting NetShield halts any current scans in process.

To exit NetShield, press ESCAPE from the Main menu. NetShield displays a confirmation prompt. Press Y to confirm that you want to exit NetShield.

Exiting NetShield in this manner has the same effect as entering the following command at the NetWare server console prompt:

```
unload netshld
```

Either way, if NetShield is configured with an unload password, you must supply the password to exit. Otherwise, typing this command will fail, and the only alternative is to switch to NetShield and exit from the Main menu. For more information, refer to "Setting the Unload Password" in Chapter 3, “Using NetShield.”

Updating NetShield Regularly

Unfortunately, new viruses (and variants of old ones) appear and circulate often in the personal computer community. Fortunately, McAfee updates the antivirus data files regularly, usually monthly, but sooner if many new viruses have appeared. Each new version may detect as many as 60–100 new viruses or more, and may add new features. For instructions on downloading McAfee updates, refer to “Contacting McAfee” in Chapter 1, “Welcome to NetShield..” To find out what is new in a downloaded release, review the accompanying README.1ST text file.

Chapter 3 Using NetShield

Once you have installed and loaded NetShield, you can begin using it to protect your network from viral infection. This chapter describes each feature in detail and shows you how to use NetShield most effectively in your network environment.

NetShield detects known viruses by searching the system for known characteristics (sequences of code) unique to each computer virus and reporting their presence if found. For viruses that encrypt or cipher their code so that every infection is different, NetShield uses detection algorithms that work by statistical analysis, heuristics, and code disassembly.

NetShield can also check for new or unknown viruses by comparing files against previously recorded validation data. For more information, refer to "Setting CRC Validation" in this chapter. If a file has been modified, it will no longer match the validation data, and NetShield will report that the file may have become infected.

NetShield can scan your system in the following ways:

- **Immediate scanning** performs a scan of your system, on demand, using current scan settings. For more information, refer to "Running an Immediate Scan" in this chapter.
- **On Access scanning** prevents infected files from being copied to or from server volumes. For more information, refer to "Using On Access Scanning" in this chapter.
- **Periodic scanning** schedules scanning for a specific day and time. For more information, refer to "Using Periodic Scanning" in this chapter.

In each case, you can determine which network volumes NetShield scans. You can use any or all of these scanning methods in combination.

If You Detect a Virus

We strongly recommend that you get experienced help in dealing with viruses if you are unfamiliar with anti-virus software and methods. This is especially true for “critical” viruses, because improper removal of these viruses can result in the loss of all data and use of the infected disks.

If you are at all unsure about how to proceed once you have found a virus, contact McAfee for assistance. Refer to “How to contact McAfee” in Chapter 1.

Configuration Recommendations

We recommend that you customize NetShield with the settings that best fit the needs of your network environment, then save settings in a configuration file so that you can load them easily in the future. For more information, refer to "Setting Configuration File Options" in this chapter.

If it finds or suspects a virus, NetShield can perform certain actions automatically, depending on how you have configured NetShield:

- NetShield can delete, move, or ignore an infected file. We recommend that you move infected files to a quarantine directory for later inspection. For more information, refer to "Setting the Infected File Action" in this chapter.
- NetShield can notify selected users and the system console of a possible infection. We recommend that you enable this feature so that system administrators are informed as soon as viruses are detected. For more information, refer to "Setting the User Contact Action" in this chapter.
- NetShield can record a virus incident in a log file. We recommend that you enable this feature so that you can use the information to investigate any viral infections that arise. For more information, refer to "Setting the Log File" in this chapter. You can view or print the contents of this log for future reference.
- For network environments requiring strict security, consider using the following features:
    - NetShield can require a password before it can be unloaded on the server. For more information, refer to "Setting the Unload Password" in this chapter.
    - NetShield can prevent users from writing to selected network directories, such as system directories containing application executable files. For more information, refer to "Configuring Network Security" in this chapter.

To optimize server performance, consider adjusting the execution priority. For more information, refer to "Setting the Delay Factor" in this chapter.

Running an Immediate Scan

NetShield can run a scan on-demand using immediate scanning. NetShield scans the server volumes you select.

From the NetShield Main menu, choose Immediate Scan. NetShield displays the Immediate Scan menu with the following options:

- Start Scan
- Stop Scan
- Edit Volume

The rest of this section describes these options in detail.

Selecting volumes to scan

Before you start checking for viruses on your network, you must first select one or more volumes to scan. You can modify the list of volumes that NetShield scans for viruses.

From the NetShield Main menu, choose Immediate Scan | Edit Volume. NetShield displays a list of currently selected volumes.

- To add a volume to the list, press INSERT. NetShield displays a list of available volumes. Highlight the volume you want to add, then press ENTER (to select multiple volumes, highlight each one and press F5 to mark it, then press ENTER). NetShield adds the selected volume(s) to the list of volumes to scan.
- To remove a volume from the list of selected volumes, highlight it, then press DELETE. The selected volume is no longer displayed in the list of volumes to scan.

Once you have selected the volumes you want to scan, you can begin scanning your system.

Running an Immediate Scan

You can tell NetShield to start scanning immediately, based on your current scan settings.

From the NetShield Main menu, choose Immediate Scan | Start Scan. NetShield starts scanning your system. To see scanning statistics, press F10: NetShield displays the name of each file it scans, as well as the name of the last virus found (if any).

Note: If NetShield finds a virus, refer to "If you detect a virus" earlier in this chapter for more information.

Interrupting a Scan in Progress

NetShield scans your system until all selected items (volumes, directories, files) have been checked for viruses. If necessary, however, you can interrupt an immediate scan in progress.

From the NetShield Main menu, choose Immediate Scan | Stop Scan. NetShield displays a confirmation prompt.

Note: When you interrupt scanning, you prevent NetShield from completely checking the selected volumes on your system for viruses. To ensure that your system is virus-free, you must run a complete, uninterrupted scan.

Configuring the Scanning Mode

In addition to immediate scanning, NetShield provides the following scanning modes:

- **On Access Scanning** prevents infected files from being copied to or from server volumes.
- **Periodic Scanning** schedules scanning for a specific day and time.

From the NetShield Main menu, choose Configure Scanning Mode. NetShield displays the Scanning Mode Configuration menu with the following options:

- On Access Scanning
    - Periodic Scanning

The rest of this section describes these scanning modes in detail.

Using On Access Scanning

If On Access scanning is enabled, NetShield can protect your server against viruses by preventing infected files from being copied to or from server volumes. If a filemask is used in the copy operation (for example, *.EXE), NetShield prevents only infected files from being copied. Use on access scanning to prevent spreading viruses in the interim between regular scans.

Note: If NetShield finds a virus, refer to "If you detect a virus" earlier in this chapter for more information.

To use on access scanning, from the NetShield Main menu, choose Configure Scanning Mode | On Access Scanning. NetShield displays the On Access Scanning menu with the following options:

- Inbound Files Only
- Outbound Files Only
- Inbound and Outbound Files
- Disable On Access Scanning

Select the option you want.

Inbound Files Only

Select this option to prevent copying infected files to the selected server volume. When a copy operation is attempted, NetShield checks the file on the target volume and, if infected, deletes, moves, or ignores the file according to the current action setting. For more information, refer to "Setting the Infected File Action" later in this chapter.

We recommended this option for most environments because it protects the server but avoids running extra scans every time files are copied from the server volume.

Outbound Files Only

Select this option to prevent copying infected files from selected server volumes to other server or workstation volumes. When a copy operation is attempted, NetShield checks the file on the source volume and, if infected, deletes, removes, or ignores the file according to the current action setting. For more information, refer to "Setting the Infected File Action" later in this chapter.

This option does not protect the server volume against infected files copied to it, and is recommended only in cases where the server volume is read-only and might contain infected files.

Inbound and Outbound Files

Select this option to prevent copying infected files to or from selected server volumes. This option combines the two previous options and offers the highest degree of protection for both servers and workstations. It may, however, result in extra scans if the server volume is highly unlikely to contain infected files.

Viewing Statistics for On Access Scanning

When you open the On Access Scanning menu, NetShield displays information similar to the following example:

```
          NetShield On Access Virus Detection Summary

Last Inbound File Scanned:
Last Outbound File Scanned:
Last Inbound Virus Detected:
Last Outbound Virus Detected:
Total Files Scanned: 360    Total Infected Files Found: 271
Current On Access Scan Mode: Both Inbound and Outbound Files
```

Disabling On Access Scanning

Select this option to disable on access scanning altogether or to interrupt an on access scan in progress. Thereafter, NetShield will not check files as they are copied to or from the server volume.

Using Periodic Scanning

You can schedule NetShield to automatically scan server volumes at a future date and time. Thereafter, NetShield runs the scan at the scheduled time *if* the server is running and NetShield is loaded and running. In this way, you can scan your network unattended, during periods of low network traffic, and thereby ensure that scanning occurs on a regular basis. For each scheduled scan, you can specify when to scan, what to scan, and which scan options to use.

Note: If NetShield finds a virus, refer to "If you detect a virus" earlier in this chapter for more information.

From the NetShield Main menu, choose Configure Scanning Mode | Periodic Scanning. NetShield displays the Periodic Scanning menu with the following options:

- Scanning
  - Day of Week
  - Day of Month
  - Time of Day
- Select Volumes to Scan
- Load Scan Settings from File
- Save Scan Settings to File

Select the option you want.

Selecting the Scanning Frequency

You can schedule scanning on a daily, weekly, or monthly basis. For the best network performance, schedule scanning during periods of low network traffic, such as at 2:00 am or on weekends.

To enable scanning, highlight **Scanning <DISABLED>** and press ENTER. NetShield displays the Select Scanning Frequency menu with the following options. Select the scanning frequency you want and enter the required information:

- **Daily**: Enter the time of day (0:01 to 23:59, in 24-hour format).
- **Weekly**: Enter the day of the week (Sunday to Saturday) and the time of day (0:01 to 23:59).
- **Monthly**: Enter the day of the month (1-31) and the time of day (0:01 to 23:59). If you enter 31, NetShield will scan on the last day of the month, even if it has fewer than 31 days.

Thereafter, NetShield runs the scan at the scheduled date and time.

Selecting Volumes for Periodic Scanning

You can select the network volumes you want to scan in periodic scanning. These apply to the periodic scan only, and do not change the currently selected volumes for immediate or on access scanning. For more information, refer to "Selecting Volumes to Scan" earlier in this chapter.

Highlight **Select Volumes To Scan** and press ENTER. NetShield displays a list of currently selected volumes.

- To add a volume to the list, press INSERT. NetShield displays a list of available volumes. Highlight the volume you want to add, then press ENTER (to select multiple volumes, highlight each one and press F5 to mark it, then press ENTER). NetShield adds the selected volume(s) to the list of volumes to scan.
- To remove a volume from the list, highlight it, press DELETE, then choose Yes when prompted to confirm deletion. NetShield removes the selected volume from the list of volumes to scan.

NetShield will scan the selected volumes in subsequent scheduled scans, including any changes you have just made.

Saving a Configuration File for Periodic Scanning

You can store NetShield scan settings that apply only to the periodic scan in a special configuration file. By default, NetShield uses SYS:\SYSTEM\PER$CFG.DAT. We recommend that you use the default path so that configuration files are easy to locate.

Configuration files for periodic scanning differ from configuration files created according to the instructions in "Setting Configuration File Options" later in this chapter. They contain only the scheduled scanning date and time, plus the volumes selected for periodic scanning.

From the Periodic Scanning menu, highlight **Save Scan Settings to File** and press ENTER. NetShield prompts you to identify the configuration file you want to save. Type the volume, path, and name of the configuration file you want, then press ENTER. Alternatively, to find the file:

1. Press INSERT to display a list of available volumes.
2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).
3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.
4. If necessary, continue selecting subdirectories until you select the one containing the configuration file you want to use.

5. Highlight the configuration file you want to use, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to accept this path and filename, or ESCAPE to abandon the operation.

NetShield prompts you to accept your changes and, if you answer Yes, saves the configuration file you specified.

Loading a Configuration File for Periodic Scanning

You can load a periodic scanning configuration file created using the instructions in the previous section, "Saving a Configuration File for Periodic Scanning." By default, NetShield uses SYS:\SYSTEM\PER$CFG.DAT.

From the Periodic Scanning menu, highlight **Load Scan Settings from File** and press ENTER. NetShield prompts you to identify the configuration file you want to load. Type the volume, path, and name of the configuration file you want, then press ENTER. Alternatively, to find the file:

1. Press INSERT to display a list of available volumes.
2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).
3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.
4. If necessary, continue selecting subdirectories until you select the one containing the configuration file you want to use.
5. Highlight the configuration file you want to use, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to accept this path and filename, or ESCAPE to abandon the operation.

NetShield prompts you to accept your changes and, if you answer Yes, loads the configuration file you specified and uses it for subsequent scheduled scans.

Disabling Periodic Scanning

You can disable periodic scanning to halt a period scan in progress or to prevent future scheduled scans.

To disable periodic scanning, highlight **Scanning**, then press ENTER. NetShield displays the Scanning Frequency list. Highlight <DISABLED>, then press ENTER.

Configuring Virus Detection

You can configure NetShield to take certain actions automatically if it finds an infected file when scanning your network. NetShield can:

- Delete, remove, or ignore infected files.
- Notify selected users and generate a message to the NetWare system console that a virus has been found.

To configure NetShield in this way, from the NetShield Main menu, choose Configure Virus Detection. NetShield displays the Virus Detect Configuration menu with the following options:

- Infected File Action
- User Contact Action

The rest of this section describes these options in detail.

Setting the Infected File Action

You can tell NetShield what to do with infected files found during a scan. NetShield can delete them to prevent further infection, move them to a quarantine directory for inspection or uploading to McAfee, or do nothing but report the infection in a log file.

From the NetShield Main menu, choose Configure Virus Detection | Infected File Action. NetShield displays the Select Action from List menu with the following options:

- Delete & Overwrite Infected File
- Move Infected File
- Ignore Infected File

Select the action you want from the list.

Deleting and Overwriting Infected Files

Select this option to delete infected files found during a scan so that they cannot be recovered except from backups. NetShield erases any infected files and writes random characters to the disk space formerly occupied by the infected file. As a result, this file is completely eradicated from your network and is not recoverable by you or other users, except from backups. This is the most secure option, but it can prevent you from recovering an infected file you might want to save for further inspection.

Moving Infected Files

Select this option to move infected files found during a scan to a different directory so that you can inspect them yourself and, if you want, upload them to McAfee for expert inspection. To avoid a situation in which users could inadvertently load an infected file and spread the virus, the directory you specify should be a "quarantine directory" to which only system administrators have access.

To specify a directory, type the volume and path of the directory you want, then press ENTER. Alternatively, to find the directory:

1. Press INSERT to display a list of available volumes.
2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).
3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.
4. If necessary, continue selecting subdirectories until you highlight the one you want to use for infected files.

5. Highlight the directory you want to use, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to select this directory.

NetShield prompts you to accept your changes and, if you answer Yes, uses the directory you selected. If the directory you specify does not exist, NetShield creates it for you automatically.

Ignoring Infected Files

Select this option to ignore infected files found during a scan. NetShield leaves any infected files intact on your system, which could result in further viral infection. We therefore recommend that you check the log files for infected files immediately after scanning and, if found, take steps to protect your system.

Warning: This option is less secure than other options. Infected files might still be copied to the server and *viruses might spread even when NetShield is active*.

Setting the User Contact Action

You can configure NetShield to send a broadcast message, e-mail message, or pager message to one or more users if infected files were found during a scan. That way, you and others can know immediately when viruses have been detected on your network. NetShield can also generate console messages to the NetWare server console.

From the NetShield Main menu, choose Configure Virus Detection | User Contact Action. NetShield displays the User Contact Actions menu.

- Edit MHS Configuration
- Edit Pager Configuration
- Edit User Contact List
- Enable User Alarms
- Enable Console Messages

Select the options you want.

Editing the MHS Configuration

Select this option to have NetShield, if a virus is detected, notify users automatically via e-mail. NetShield gets messages to network administrators and support personnel using Novell's Message Handling Service (MHS), which can route e-mail messages throughout your network and via mail gateways to external mail services.

Note: To use this feature, you must have Novell Basic or Global MHS installed and running on your network, and you must have a list of possible recipients defined within your MHS setup.

If NetShield detects a virus during volume scanning, NetShield sends mail notifications once to selected users after scanning is concluded. If on access scanning is enabled (refer to "Using On Access Scanning" earlier in this chapter), however, NetShield sends a notification as soon as a virus is detected. For example, if a user copies 20 infected files, NetShield notifies active users with 20 different messages in rapid succession. To prevent a backlog of redundant messages, you can set a Minimum Notification Interval (MNI), in minutes, that NetShield will wait before sending a new notification. For example, if the MNI is set to 5 and all 20 infected files are copied within 5 minutes, NetShield sends only one message. If it takes 16 minutes to copy all 20 files, NetShield sends 3 rounds of messages.

From the User Contact Actions menu, choose **Edit MHS Configuration**. NetShield displays the MHS Configuration menu with the following options:

- Edit Master MHS User List
- Edit Active MHS User List
- Edit MHS Server Configuration
- Send Test Mail to Active List Members
- MHS Alert Status

Select the options you want.

Editing the Master MHS User List

You can create a master list of likely recipients of NetShield notifications, such as network administrators or support staff. You use this list to select active MHS recipients, as described in "Editing the Active MHS User List" later in this section.

To specify users in the master list, highlight **Edit Master MHS List** and press ENTER. NetShield displays a list of possible MHS recipients.

- To add a user to the list, press INSERT. NetShield displays a list of available users. Highlight the user you want to add, then press ENTER. NetShield adds the selected user to the master MHS user list.

NetShield obtains the recipient's name and mail address. Specify a Minimum Notification Interval for the user, if you want, or leave it unchanged to use the default interval defined in "Editing the MHS Configuration" later in this section.

- To remove a user from the list, highlight it, then press DELETE. NetShield deletes the selected user from the master MHS user list.

Editing the Active MHS User List

From the master list of MHS users, you can select the users that NetShield will notify automatically if a virus is detected. To specify the users to notify, highlight **Edit Active MHS User List** and press ENTER. NetShield displays a list of users to notify (this list is initially empty).

- To add a user to the list, press INSERT. NetShield displays the master MHS user list. Highlight the user you want to add, then press ENTER. NetShield adds the selected user to the list of users to notify.
- To remove a user from the list, highlight it, then press DELETE. NetShield deletes the selected user from the list of users to notify.

NetShield will notify the users on this list, not on the master MHS list.

Editing the MHS Configuration

You must supply NetShield with certain information needed to communicate via MHS. Choose **Edit the MHS Configuration** and enter the following information.

- **MHS Server Name**, which is the name of the server running the MHS service
- MHS Server **User Name**, which is a valid user name for the MHS server. NetShield uses this when connecting to the MHS server.
- MHS Server **Password** associated with the MHS Server User Name entered above.
- **Minimum Mail Interval** for NetShield to use when it is not specified for an active user.

Press ENTER to save your changes, or ESC to exit without saving them.

Sending Test Mail to Active List Members

To verify your current MHS settings, we recommend that you send test mail to users on the active list. Choose **Send Test Mail to Active List Members**, and NetShield will send a message to every user on the list.

Setting the MHS Alert Status

Select this option to activate or disable the MHS alert feature. To change the current setting, highlight **MHS Alert Status**, press ENTER, then choose <ENABLED> or <DISABLED> from the prompt.

Editing the Pager Configuration

Select this option to have NetShield, if a virus is detected, notify users immediately via pagers. NetShield dials standard pager numbers and sends your message to selected network administrators and support personnel.

Note: To use this feature, you must have a Hayes-compatible modem installed, running, and accessible on your NetShield server.

If NetShield detects a virus during volume scanning, NetShield sends page notifications once to selected users after scanning is concluded. If on access scanning is enabled (refer to "Using On Access Scanning" earlier in this chapter), however, NetShield sends a notification as soon as a virus is detected. For example, if a user copies 20 infected files, NetShield notifies active users with 20 different pages in rapid succession. To prevent a backlog of redundant pager notifications, you can set a Minimum Notification Interval (MNI), in minutes, that NetShield will wait before sending a new notification. For example, if the MNI is set to 5 and all 20 infected files are copied within 5 minutes, NetShield sends only one pager notification. If it takes 16 minutes to copy all 20 files, NetShield sends 3 rounds of pager notifications.

If NetShield cannot get a dial tone for the configured modem, it waits 3 minutes and retries. After 3 unsuccessful attempts, NetShield displays an error message on screen and, if enabled, displays it on the server console and writes it to the log file.

From the User Contact Actions menu, choose **Edit Pager Configuration**. NetShield displays the Pager Configuration menu with the following options:

- Edit Master Pager User List
- Edit Active Pager User List
- Edit Pager Configuration
- Test Selected Pagers
- Pager Alert Status

Select the options you want.

Editing the Master Pager User List

You can create a master list of likely recipients of NetShield notifications, such as network administrators or support staff. You use this list to select active pager recipients, as described in "Editing the Active Pager List" later in this section.

To specify users in the master list, highlight **Edit Master Pager List** and press ENTER. NetShield displays a list of possible pager recipients (this list is initially empty).

- To add a user to the list, press INSERT. NetShield displays Enter Pager Record menu. Enter the name of the person to page, their Minimum Notification Interval (optional), and a dial string, which has the following format:
  - **Dial Prefix**, such as 9 to get an outside line (required for some phone systems)
  - **Area Code**
  - **Phone Number (without hyphens, periods, or parentheses)**
  - **Delay**, using commas, which sets a 2-second delay per comma (required by some pager services, and varying from service to service).
  - **Personal Identification Number (PIN) (required by some pager services)**
  - **Message (up to 40 characters)**

  Here is an example dial string:

  9,1,8007597243,,,9999999#,,,222#,#

  This string dials 9 to get an outside line, dials an 800 number, pauses for 6 seconds, enters a PIN (of 9999999), pauses another 6 seconds, enters a message of "222" that terminates with the pound sign (#, which is required for some pager services, waits 2 seconds, and terminates the call with the pound sign (again, required for some pager services).

  Press ENTER to save your changes, or ESC to exit without saving them.
- To remove a user from the list, highlight it, then press DELETE. NetShield deletes the selected user from the master pager list.

Editing the Active Pager User List

From the master list of pagers, you can select the users that NetShield will notify automatically if a virus is detected. To specify the users to notify, highlight **Edit Active Pager User List** and press ENTER. NetShield displays a list of users to notify (this list is initially empty).

- To add a user to the list, press INSERT. NetShield displays the master pager list. Highlight the user you want to add, then press ENTER. NetShield adds the selected user to the list of users to notify.

- To remove a user from the list, highlight it, then press DELETE. NetShield deletes the selected user from the list of users to notify.

NetShield will notify the users on this list, not on the master pagers list.

Editing the Pager Configuration

You must supply NetShield with certain information needed to communicate with pagers via modem. Choose **Edit the Pager Configuration** and enter the following information:

- **Communications Board Number**, as defined by the AIOCOMX.NLM utility, which determines the board number of the modem installed on your NetShield server machine.
- **Port Number**, as defined by the AIOCOMX.NLM utility, which determines the port number of the modem installed on your NetShield server machine.
- **Minimum Notification Interval** for NetShield to use when it is not specified for an active user.

Press ENTER to save your changes, or ESC to exit without saving them.

Sending a Test Page to Active List Members

To verify your current pager settings, we recommend that you send a test page to users on the active list. Choose **Send Test Page to Active List Members**, and NetShield will send a message to every pager on the list.

Setting the Pager Alert Status

Select this option to activate or disable the pager alert feature. To change the current setting, highlight **Pager Alert Status**, press ENTER, then choose <ENABLED> or <DISABLED> from the prompt.

Editing the User Contact List

You can have NetShield notify certain users via a broadcast if viruses have been found. To specify the users to notify, highlight **Edit User Contact List** and press ENTER. NetShield displays a list of users to notify.

- To add a user to the list, press INSERT. NetShield displays a list of available network users. Highlight the user you want to add, then press ENTER. NetShield adds the selected user to the list of users to notify.
- To remove a user from the list, highlight it, then press DELETE. NetShield deletes the selected user from the list of users to notify.

NetShield will notify the users on this list if viruses are found in future scans, including any changes you have just made.

Enabling User Alarms

You can tell NetShield whether to inform selected users that infected files were found during a scan. You might want to disable this capability if, for security reasons, you do not want users to know that viruses have been found. However, if you disable this feature, be sure to inspect the log file immediately after each scan so that you know whether your network has been infected.

To change the current setting, highlight **Enable User Alarms**, type Y (for Yes) or N (for No), then press ENTER

Enabling Console Messages

You can tell NetShield whether to display messages about infected files on the NetWare system console. This provides an alternative method for alerting system administrators and maintains an audit trail for further investigation into virus incidents. For more information about NetWare server console messages, refer to your NetWare documentation.

To change the current setting, highlight **Enable Console Messages**, type Y (for Yes) or N (for No), then press ENTER

Configuring NetShield NLM

You can configure NetShield to:

- Save and load configuration files containing frequently-used NetShield settings.
- Exclude directories from scanning.
- Regulate server performance by assigning CPU processing priority to NetShield.
- Perform CRC validation to detect new or unknown viruses.
- Perform cross-server updating of NetShield data files
- Protect NetShield from unauthorized unloading by assigning a password.

From the NetShield Main menu, choose Configure NetShield NLM. NetShield displays the NetShield NLM Configuration menu with the following options:

- Configuration File Options
- Configure Excluded Directories
- NetShield Delay Factor
- CRC Configuration Options
- Password Configuration
- Edit Cross-Server Updating

The rest of this section describes these options in detail.

Setting Configuration File Options

You can store current NetShield configuration information in a disk file that you can later load as needed. You can also obtain a copy of the current configuration settings by printing a report or saving them to an ASCII text file.

A NetShield configuration file stores configuration information in a proprietary binary format and contains settings information such as the selected volumes to scan, periodic scan settings, logging, CRC checking, and other NetShield settings (you can print a list of current settings). Passwords are encrypted.

From the NetShield Main menu, choose Configure NetShield NLM | Configuration File Options. NetShield displays the Configuration File Management Options menu with the following options:

- Load Configuration Settings From File
- Save Configuration Settings To File

- Write Configuration Report To File
- Print Current Configuration Settings

Select the options you want.

Loading Configuration Settings from a File

Select this option to load a configuration file from disk. NetShield prompts you to identify the configuration file you want to load. By default, NetShield uses SYS:\SYSTEM\VIR$CFG.DAT. We recommend that you use the default path so that the configuration files are easy to locate if you need to investigate a problem.

Type the volume, path, and name of the configuration file you want, then press ENTER. Alternatively, to find the file:

1. Press INSERT to display a list of available volumes.
2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).
3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.
4. If necessary, continue selecting subdirectories until you select the one containing the configuration file you want to use.
5. Highlight the configuration file you want to use, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to accept this filename, or ESCAPE to abandon the operation.

NetShield prompts you to accept your changes and, if you answer Yes, loads the configuration file you specified and uses it for subsequent scans.

Saving Configuration Settings to a File

Select this option to save a configuration file to disk. NetShield prompts you to identify the name and path of the configuration file you want to save. By default, NetShield uses SYS:\SYSTEM\VIR$CFG.DAT. We recommend that you use the default path so that the configuration files are easy to locate if you need to investigate a problem.

Type the volume, path, and name of the configuration file you want, then press ENTER. Alternatively, to find the file:

1. Press INSERT to display a list of available volumes.
2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).

3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.
4. If necessary, continue selecting subdirectories until you select the one containing the configuration file you want to use.
5. Highlight the configuration file you want to use, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to accept this filename, or ESCAPE to abandon the operation.

NetShield prompts you to accept your changes and, if you answer Yes, writes configuration information to the file you specified.

Writing the Configuration Report to a File

Select this option to save the configuration report in an ASCII text file. NetShield prompts you to identify the name and path of the report file you want to create. By default, NetShield uses SYS:\SYSTEM\VIR$CFG.RPT. We recommend that you use the default path so that report files are easy to locate.

Type the volume, path, and name of the report file you want, then press ENTER. Alternatively, to find the file:

1. Press INSERT to display a list of available volumes.
2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).
3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.
4. If necessary, continue selecting subdirectories until you select the one containing the configuration file you want to use.
5. Highlight the configuration file you want to use, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to accept this filename, or ESCAPE to abandon the operation.

NetShield prompts you to accept your changes and, if you answer Yes, writes configuration information to the report file you specified. If the report file exists, NetShield overwrites it.

Printing Current Configuration Settings

Select this option to send a report of the current configuration settings to a network printer queue. NetShield displays a list of available print queues. Highlight the queue you want, then press ENTER to select it. NetShield sends the report to the queue you selected.

Configuring Excluded Directories

You can exclude selected directories from scanning if you want to reduce scanning time and you are confident that such directories are unlikely to be infected by a virus. For example, because most viruses infect executable files, you might want to exclude directories that contain only data files.

From the NetShield Main menu, choose Configure NetShield NLM | Configure Excluded Directories. NetShield displays the Configure Excluded Directories menu with the following options:

- Edit List of Excluded Directories
- Apply Exclusion List to All Scans

The rest of this section describes these options in detail.

Selecting Directories to Exclude

Select this option to change the list of directories to exclude from scanning. To specify a directory to exclude, type the volume and path of the directory you want, then press ENTER. Alternatively, to find a directory:

1. Press INSERT to display a list of available volumes.
2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).
3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.
4. If necessary, continue selecting subdirectories until you highlight the one you want to use for infected files.
5. Highlight the directory you want to use, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to select this directory.

NetShield prompts you to accept your changes and, if you answer Yes, adds the selected directory to the list of excluded directories.

To remove a directory from the list, highlight it, then press DELETE. NetShield deletes the selected directory from the list of directories to exclude.

If the exclusion list is enabled (for more information, refer to the next section), NetShield will exclude directories from scanning using this list, including any changes you have just made.

Applying the Exclusion List to All Scans

Select this option to ignore, during scanning, the directories in the exclusion list. To change the current setting, highlight **Apply Exclusion List to All Scans**, press ENTER, then choose <ENABLED> or <DISABLED> from the prompt.

Setting the Delay Factor

You can regulate server performance during scanning by controlling the amount of CPU time that NetShield uses to conduct the scan. The lower the delay, the more CPU time is devoted to carrying out the scan operation.

From the NetShield Main menu, choose Configure NetShield NLM | NetShield Delay Factor. NetShield prompts you to enter a priority. The default delay factor is 3. Type a number between 1 and 100, inclusive, then press ENTER.

- If you choose a delay setting of 1, which is the most CPU-intensive, 40–50% CPU usage is added and approximately one file is scanned per second. We recommend using higher settings during periods of low network traffic.
- If you choose a delay setting of 100, which is the least CPU-intensive, 1–2% CPU usage is added and one file is scanned approximately every 10 seconds. We recommend using lower settings during periods of high network traffic.

NetShield uses the delay factor you specified.

Setting CRC Configuration Options

If your environment is highly vulnerable to viruses, or you require additional security against them, you can use NetShield's CRC (Cyclic Redundancy Check) checking option to detect infection by new and unknown viruses. NetShield can assign validation codes to files, then use those codes to detect file changes and warn that infection by an unknown virus may have occurred. NetShield stores validation information in an encrypted database file.

The use of CRC validation codes requires an ongoing effort to store and maintain the codes. For example, if you install new programs or upgrade old ones, you should remove all the validation codes, then add them again to restore them. If you install new software, or upgrade your DOS or NetWare version, remember to update your recovery file.

Because the validation codes will change whenever a file is updated, we recommend using CRC checks only in stable environments where few software updates are performed. In addition, consider excluding any directories containing data files that are frequently updated. To exclude directories from scanning, refer to “Configuring Excluded Directories” earlier in this chapter.

Warning: Some programs are self-modifying or self-checking (most programs that do this will tell you to turn off your anti-virus software before running them). Such software deliberately changes its own program file, often to protect against viruses or illegal copying, and is therefore difficult to validate in conventional ways.

If you use NetShield's CRC validation checking, these programs can trigger a false alarms, and NetShield may report a virus in a file that is not infected. To prevent this from occurring, be sure to exclude directories containing these files, as described in "Configuring Excluded Directories" earlier in this chapter.

From the NetShield Main menu, choose Configure NetShield NLM | CRC Configuration Options. NetShield displays the CRC Configuration Options menu with the following options.

- Add CRC Code To External File
- Verify CRC Code From External File
- Remove CRC Code From External File
- Edit External File Name

Select the options you want.

Note: You can enable only one of the options (Add, Verify, and Remove) at a time during a scan. If you enable one option, NetShield automatically disables any other enabled option.

Adding CRC Code to an External File

Select this option to tell NetShield to add CRC validation codes to the external database file during the next scan. Any previous validation codes should be removed from the selected database file before proceeding. We recommend disabling this option once the validation codes have been added.

To change the current setting, highlight **Add CRC Code To External File**, press ENTER, then choose <ENABLED> or <DISABLED> from the prompt.

Verifying CRC Code from an External File

Once you have added CRC validation codes to the database, select this option to tell NetShield to check for validation codes in subsequent scans and, if files have changed, to warn that infection by an unknown virus may have occurred.

To change the current setting, highlight **Verify CRC Code From External File**, press ENTER, then choose <ENABLED> or <DISABLED> from the prompt.

Removing CRC Code from an External File

Once you have added CRC validation codes to the database, select this option to tell NetShield to remove them during the next scan from the selected database file. You normally do this if you have added or upgraded software on your network and need to re-add validation codes.

To change the current setting, highlight **Remove CRC Code From External File**, press ENTER, then choose <ENABLED> or <DISABLED> from the prompt.

Selecting the Name of the External File

By default, the database file used to store CRC validation codes is named VIR$CRC.DAT, which is stored in the same directory as the NETSHLD.NLM file. You can change the name and location of the database file as needed.

Type the volume, path, and name of the validation database file you want, then press ENTER. Alternatively, to find the file:

1. Press INSERT to display a list of available volumes.
2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).
3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.
4. If necessary, continue selecting subdirectories until you select the one containing the validation database file you want to use.
5. Highlight the database validation file you want to use, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to accept this filename, or ESCAPE to abandon the operation.

NetShield prompts you to accept your changes and, if you answer Yes, uses the validation database file you specified.

Setting the Unload Password

You can assign a password to NetShield to ensure that only authorized users can unload NetShield once it has been loaded. The password is not case-sensitive, can be up to 40 characters long, and can be any mix of alphanumeric and punctuation characters. The default NLM password is: `NETSHIELD`. The password is encrypted.

From the NetShield Main menu, choose Configure NetShield NLM | Password Configuration. NetShield displays the Password Configuration menu with the following options:

- Change Existing Password

- Password Enable Status

The rest of this section describes these options in detail.

Changing the Existing Password

Select this option to add a change the unload password. Enter the current password, if any, then enter the new password (or leave it blank to remove the password). Be sure to write down your new password and store it in a secure location.

Enabling the Unload Password

Select this option to force users to enter the unload password before exiting NetShield. To change the current setting, highlight **Password Enable Status**, press ENTER, then choose <ENABLED> or <DISABLED> from the prompt.

Using Cross-Server Updating

McAfee releases updates of the NetShield data files (SCAN.DAT and NAMES.DAT) regularly, usually monthly, to detect new viruses and variants of old ones. When you download updates of NetShield data files from McAfee, you can use NetShield's cross-server updating feature to automatically upgrade NetShield data files everywhere NetShield is installed on your network. Cross-server updating saves you the effort of performing this task manually for each server.

For cross-server updating to work for all NetShield servers on your network, you must enable it for each NetShield installation. Once enabled, NetShield periodically sends a message to other servers, via NetWare's Service Advertising Protocol (SAP), that requests each server to indicate its version of the data files. NetShield retrieves these messages from other servers and, if another NetShield installation has a more recent version of the data files, obtains these files immediately from the other installation. In this way, you can update the date files on one server and have them propagate automatically to all servers.

To change the current cross-server update settings, from the NetShield Main menu, choose Configure NetShield NLM | Edit Cross-Server Updating. NetShield displays the Edit Cross-Server Updating menu with the following options:

- Set Frequency
- Cross-Server Update Status

To set the frequency with which NetShield will query other NetShield installations for their data file versions, choose Set Frequency and enter the time interval, in minutes (up to 25 minutes). For example, if you entered 10, NetShield would query other servers every ten minutes.

To activate or disable cross-server updating, choose Cross-Server Update Status, then choose <ENABLED> or <DISABLED> from the prompt.

For more information about NetShield updates, refer to “Updating NetShield Regularly” in Chapter 2, “Installation and Setup.”

Configuring Virus Reporting

NetShield can keep a log of scans and infections found. You can view this log on screen, print it, or discard it. We recommend that you use NetShield's logging feature so that you have an audit trail to assist in your investigation of virus incidents.

From the NetShield Main menu, choose Configure Virus Reporting. NetShield displays the Virus Reporting Options menu with the following options.

- Configure Log File Settings
- Select Log File Reports

The rest of this section describes these options in detail.

Setting Up the Log File

NetShield can record the results of scanning (immediate, on access, and periodic scans) in a log file that you can later use for auditing your system and investigating problems. NetShield appends log information in the log file, including the date and time the scan was run and, if viruses are detected, an entry for each file suspected to contain a virus (name, location, and virus name).

From the NetShield Main menu, choose Configure Virus Reporting | Configure Log File Settings. NetShield displays the Log File Configuration Options menu with the following options:

- Enter Log File Path
- Enable Logging To Log File

Entering the Log File Path

Select this option to specify the name and location of the log file. If the log file has not been configured, the default filename is VIR$LOG.DAT.

Type the volume, path, and name of the log file you want, then press ENTER. Alternatively, to find the file:

1. Press INSERT to display a list of available volumes.

2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).
3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.
4. If necessary, continue selecting subdirectories until you select the one containing the log file you want to use.
5. Highlight the log file you want to use, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to accept this filename, or ESCAPE to abandon the operation.

NetShield prompts you to accept your changes and, if you answer Yes, uses the log file you specified. If the file does not exist, NetShield creates it automatically. If the file exists, NetShield prompts you to overwrite the file or append new information to it.

Enabling Logging to a Log File

We recommend that logging is enabled whenever you scan so that you have an audit trail of infections found. If necessary, you can disable logging by selecting this option.

To change the current setting, highlight **Enable Logging to a Log File**, press ENTER, then choose <ENABLED> or <DISABLED> from the prompt.

Selecting Log File Reports

If logging is enabled, NetShield can display, print, or discard the contents of the currently selected log file.

From the NetShield Main menu, choose Configure Virus Reporting | Select Log File Reports. NetShield displays the Select Log File Reports menu with the following options:

- View Contents of Log File
- Print Contents of Log File

Select the options you want.

Viewing the Log

Select this option to display the current log file and peruse its contents in a scrollable window.

Use these keys to navigate the scrollable window:

- HOME moves the cursor to the beginning of the line.

- END moves the cursor to the end of the line.
- PGUP and PGDN to view the log file one screen at a time.
- ESCAPE to exit the scrollable window.

Printing the Log

Select this option to print the current log file for future reference. NetShield displays a list of available print queues. Highlight the queue you want, then press ENTER to select it. NetShield sends the log report to the queue you selected and displays a message verifying that the report was sent.

Configuring Network Security

For highly secure networks, NetShield can detect and log any attempts to write to read-only directories, such as directories containing application executables. This log provides additional information about possible sources of viral infection on your network.

You can also suspend read-only protection for authorized users to make changes to monitored directories, such as installing or upgrading software. Password protection ensures centralized control over access to these directories.

To use network security, you configure NetShield by selecting the directories, file extensions, and users to monitor, then you activate network security monitoring.

Entering a Password

Network security is password-protected to ensure that only authorized users have access. The default password is:

```
login admin
```

You should change this password when you run NetShield for the first time. For instructions, refer to "Changing the Network Security Password" later in this section.

From the NetShield Main menu, choose Configure Network Security. NetShield prompts you to enter a password. Type the password (which is not case-sensitive), then press ENTER. NetShield displays the Configure Network Security menu with the following options:

- Edit Network Security Configuration
- Set Path for Log File
- Save Current Configuration To A File
- Restore Current Configuration From A File
- Current Network Security Status

The rest of this section describes these options in detail.

Editing the Network Security Configuration

You can configure NetShield to:

- Monitor disk write attempts for files with specific extensions.
- Monitor specific directories for write attempts.
- Exclude files from monitoring

- Monitor selected administrators for write attempts.
- Permit only selected users to write to monitored directories.

You can also save and load configuration settings in a file. For more information, refer to "Saving the Current Configuration" and "Loading a Configuration" later in this chapter.

From the NetShield Main menu, choose Configure Network Security | Edit Network Security Configuration. NetShield displays the Network Security Configuration Options menu with the following options:

- Create File and Extension Master List
- Select Entries To Monitor From Master List
- Select Files to be Excluded from Monitoring
- Select Directories To Monitor for All Users
- Change Monitored Users
- Change Temporary Authorization
- Change Network Security Password

Select the options you want.

Creating a Master List of Files and File Extensions

Select this option to manage the master list of files and file extensions to monitor. For example, you might want NetShield to monitor all executable files by adding the COM, EXE, SYS, BIN, OVL, or DLL extensions to the list. You will use this master list in the next section, "Selecting Entries to Monitor."

From the Configure Network Security menu, choose Edit Network Security Configuration | Create File and Extension Master List. NetShield displays the current master list.

- To add an extension to the list, press INSERT, type a period (required) and a new extension (up to 3 letters), then press ENTER. NetShield adds the new extension to the master list. If you want NetShield to monitor this extension, however, you must add it to another list. For more information, refer to the next section "Selecting Entries to Monitor."
- To add a file to the list, press INSERT, type the full file name (name, period, and extension), then press ENTER. NetShield adds the new file to the master list. If you want NetShield to monitor this file, however, you must add it to another list. For more information, refer to the next section "Selecting Entries to Monitor."

- To remove a file or files extension from the list, highlight it, then press DELETE. NetShield deletes the selected entry.

Once you have selected the extensions you want for the master list, you must then select the extensions you want NetShield to monitor while scanning.

Selecting Entries to Monitor

From the master list of files and file extensions, you can select the list of entries that NetShield will monitor for unauthorized write attempts. At a minimum, consider specifying standard executable file extensions (EXE, COM, SYS, BIN, OVL, and DLL). When a file is copied to a monitored directory, NetShield determines whether the copied file or its extension exists in the list of monitored entries and, if so, NetShield creates a entry in the log file.

From the Configure Network Security menu, choose Edit Network Security Configuration | Select Entries To Monitor From Master List. NetShield displays the current list of monitored files and file extensions.

- To add an entry to the list, press INSERT. NetShield displays the master list of available files and file extensions. Highlight the entry you want, then press ENTER. NetShield adds the new entry to the list of entries to monitor.
- To remove an entry from the list, highlight it, then press DELETE. NetShield deletes the selected entry from the list of entries to monitor. However, deleting it from this list does not remove it from the master list.

NetShield will monitor files with the selected name or extension in the list, including any changes you have just made.

Selecting Files to be Excluded from Monitoring

You can exclude certain files and file extensions from monitoring, such as a backup file that is frequently updated.

From the Configure Network Security menu, choose Edit Network Security Configuration | Select Files To Be Excluded From Monitoring. NetShield displays the current list of excluded files.

To specify a file or file extension to exclude from monitoring, type its name, path, and extension, then press ENTER. Alternatively, to find a file:

1. Press INSERT to display a list of available volumes.
2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).
3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.

4. If necessary, continue selecting subdirectories until you highlight the one you want to exclude.
5. Highlight the file you want to exclude, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to select this directory.

NetShield prompts you to accept your changes and, if you answer Yes, adds the selected directory to the list of directories to monitor.

To remove a directory from the list, highlight it, then press DELETE. NetShield deletes the selected directory from the list of directories to monitor.

NetShield will exclude from monitoring the files and file extensions you selected.

Selecting Directories to Monitor for All Users

You can select the directories that NetShield will protect and monitor for unauthorized write attempts. For example, you might want to monitor directories that contain application executables.

From the Configure Network Security menu, choose Edit Network Security Configuration | Select Directories To Monitor for All Users. NetShield displays the current list of monitored directories.

To specify a directory to include, type the volume and path of the directory you want, then press ENTER. Alternatively, to find a directory:

1. Press INSERT to display a list of available volumes.
2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).
3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.
4. If necessary, continue selecting subdirectories until you highlight the one you want to use for monitored files.
5. Highlight the directory you want to use, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to select this directory.

NetShield prompts you to accept your changes and, if you answer Yes, adds the selected directory to the list of directories to monitor.

To remove a directory from the list, highlight it, then press DELETE. NetShield deletes the selected directory from the list of directories to monitor.

NetShield will monitor directories using this list, including any changes you have just made.

Changing Monitored Users

You can select the administrators that NetShield will restrict for write attempts to all volumes and directories. From the Configure Network Security menu, choose Edit Network Security Configuration | Change Monitored Users.

NetShield displays the list of currently restricted users.

- To add a user to the list, press INSERT. NetShield displays a list of available users, as shown in the following example:

  ```
  <SystemAdministrators>
  {UsersNotInAnyGroups}
  [EVERYONE]
  [WORDPROCESSING]
  ```

  Highlight a group, then press ENTER. NetShield displays a list of users for that group. Highlight a user you want to restrict, then press ENTER. NetShield adds the selected user to the list of restricted users.

- To remove a user from the list, highlight it, then press DELETE. NetShield deletes the selected user name from the list of restricted users.

NetShield will monitor only users and groups in this list, including any changes you have just made.

Authorizing Temporary Access to Monitored Directories

You can suspend, for a brief time, read-only protection on monitored directories so that authorized users can make changes. For example, you might want to allow one or more administrators to install or upgrade software in a monitored directory.

From the Configure Network Security menu, choose Edit Network Security Configuration | Change Temporary Authorization. NetShield displays the Change Temporary Authorization menu with the following options:

- Change Temporary Authorization List
- Enable Administrative Access

Select the options you want.

Specifying Temporary Authorized Administrators

Select this option to allow certain administrators to write to monitored directories during temporary authorization. You select from the list of monitored users. For more information, refer to the previous section, "Changing Monitored Users."

From the Configure Network Security menu, choose Edit Network Security Configuration | Change Temporary Authorization | Change Temporary Authorization List. NetShield displays the list of currently monitored users.

- To add a monitored user to the temporary authorization list, press INSERT. NetShield displays a list of monitored users. Highlight a user, then press ENTER. NetShield adds the selected user to the list of temporarily authorized administrators.
- To remove a user from the list, highlight it, then press DELETE. NetShield deletes the selected user name from the list of temporarily authorized administrators.

NetShield will permit access to protected directories only to users in this list, including any changes you have just made.

Enabling Administrative Access

Select this option to allow authorized administrators to write to a protected directory while network security monitoring is enabled. You might want to do this, for example, to install or upgrade software stored in a monitored directory.

From the Configure Network Security menu, choose Edit Network Security Configuration | Change Temporary Authorization | Enable Administrative Access. NetShield prompts you to enter the number of minutes you want to enable access.

- To enable access, type a number between 1 and 180, inclusive, then press ENTER. NetShield displays the time remaining for authorized administrators to update monitored directories.

Note: If the administrative access time runs out while changes are being made to monitored directories, NetShield completes the current write operation, if any, then prevents additional changes.

- To disable access, enter 0, the default access time.

Changing the Network Security Password

You can assign a password to NetShield to ensure that only authorized users can access network security. The password is not case-sensitive, can be up to forty (40) characters long, and can be any mix of alphanumeric and punctuation characters. The password is encrypted.

From the Configure Network Security menu, choose Edit Network Security Configuration | Change Network Security Password. Enter the current password, if any, then enter the new password. Be sure to write down your new password and store it in a secure location.

Setting Up the Log File

NetShield can record the results of network security monitoring in a log file that you can later use for auditing your system and investigating problems. NetShield appends the following information in the log file: the date and time of the attempt as well as the user, workstation, file, and target directory involved.

Here is a sample entry in the log file:

```
Wed Aug 31 17:09:14 1994
      Attempt to write file XXX.EXE to
      directory SYS:\SYSTEM\
      on server STORM by user SUPERVISOR, ID 1
      From Workstation  0000001C/0000c0cf0400
DENIED!
```

From the Configure Network Security menu, choose Set Path for Log File. NetShield prompts you to specify the log file name and path. If the log file has not been configured, the default filename is NETSHLD.LOG.

Type the volume, path, and name of the log file you want, then press ENTER. Alternatively, to find the file:

1. Press INSERT to display a list of available volumes.
2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).
3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.
4. If necessary, continue selecting subdirectories until you select the one containing the log file you want to use.
5. Highlight the log file you want to use, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to accept this filename, or ESCAPE to abandon the operation.

NetShield prompts you to accept your changes and, if you answer Yes, uses the log file you specified. If the file does not exist, NetShield creates it automatically.

Saving the Current Configuration

Select this option to save the network security configuration file to disk. NetShield prompts you to identify the name and path of the configuration file you want to save. By default, NetShield uses SYS:\SYSTEM\NETSHLD.CFG. We recommend that you use the default path so that the configuration files are easy to locate if you need to investigate a problem.

Note: The network security configuration file contains information about your network security setup, not about your NetShield virus protection configuration.

From the Configure Network Security menu, choose Save Current Configuration to a File. NetShield prompts you to identify the name and path of the configuration file you want to save. By default, NetShield uses SYS:\SYSTEM\NETSHLD.CFG. We recommend that you use the default path so that the configuration files are easy to locate if you need to investigate a problem.

Type the volume, path, and name of the network security file you want, then press ENTER. Alternatively, to find the file:

1. Press INSERT to display a list of available volumes.
2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).
3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.
4. If necessary, continue selecting subdirectories until you select the one containing the configuration file you want to use.
5. Highlight the configuration file you want to use, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to accept this filename, or ESCAPE to abandon the operation.

NetShield prompts you to accept your changes and, if you answer Yes, writes configuration information to the configuration file you specified.

Restoring a Configuration from a File

Select this option to load a network security configuration file from disk.

From the Configure Network Security menu, choose Save Restore Current Configuration from a File. NetShield prompts you to identify the name and path of the configuration file you want to save. By default, NetShield uses SYS:\SYSTEM\NETSHLD.CFG. We recommend that you use the default path so that the configuration files are easy to locate if you need to investigate a problem.

Type the volume, path, and name of the configuration file you want, then press ENTER. Alternatively, to find the file:

1. Press INSERT to display a list of available volumes.
2. Highlight the volume you want, then press ENTER. NetShield displays a list of directories (directory names are enclosed in square brackets).
3. Highlight the directory you want, then press ENTER. NetShield displays a list of subdirectories, files, or both.

4. If necessary, continue selecting subdirectories until you select the one containing the configuration file you want to use.
5. Highlight the configuration file you want to use, then press ESCAPE. NetShield displays the volume, path, and filename you selected.
6. Press ENTER to accept this filename, or ESCAPE to abandon the operation.

NetShield prompts you to accept your changes and, if you answer Yes, loads the configuration file you specified and uses it for subsequent monitoring.

Enabling Network Security

Select this option to activate or disable NetShield's network security feature.

To change the current setting, on the Configure Network Security menu, highlight **Current Network Security Status**, press ENTER, then choose <ENABLED> or <DISABLED> from the prompt.

Index

I

L

M

N

O

P

R

S

T

U

V

W