

Contents

The following Help Topics are available:

Welcome to NetShield

[What is NetShield?](#)

[Starting NetShield](#)

[Updating NetShield](#)

[Configuring NetShield for Your Network](#)

[If You Detect a Virus](#)

[How Do I...?](#)

Configuration Options

[Scanning Options](#)

[Notification Options](#)

[Security Options](#)

NetShield Console

[NetShield Configuration Window](#)

[Scanning property page](#)

[Notification property page](#)

[Scanning property page](#)

[Menu Bar](#)

[Tool Bar](#)

[Status Bar](#)

For Help on Help, Press F1

What is NetShield?

NetShield is a powerful tool for the detection of viruses on your network. With new viruses and virus strains appearing every day, network security has become a critical responsibility for network administrators. NetShield allows you to protect your network from viral infections from any source - workstation, bridge, or modem. And because NetShield is a NetWare Loadable Module (NLM), you can integrate it easily into your NetWare environment, allowing it to function independently of any workstation.

Scanning Options

- **On Demand Scanning.** NetShield can scan volumes of attached servers for viruses on demand. See [Scan Server Now](#).
- **On Access Scanning.** NetShield can watch for viruses as users copy files to and from your network. See [On Access Scanning](#).
- **Periodic Scanning.** NetShield can check your network at regular intervals. See [Daily Scanning](#), [Weekly Scanning](#), or [Monthly Scanning](#).
- **CRC Scanning.** NetShield can even find new or undiscovered viruses using CRC (Cyclic Redundancy Check) scanning. See [CRC Options](#).

Security Options

- **Monitor Write Access.** Restrict write access to specific files, extensions, directories or users. You can also save unauthorized write attempts to a log file. See [Monitoring](#).
- **Exclude Files From Monitoring.** You can exclude specific files from monitoring, such as backup files or data files that are frequently updated. See [Exclude Files](#).
- **Temporary Authorization.** Suspend, for a limited time, read-only protection on monitored files, extensions, directories or users. See [Temporary Authorization](#).

Notification Options

- **User Alert.** Notify selected users when a virus is detected through a broadcast message, GMHS E-mail, console message or even by calling your pager. See [Configure User Alerts](#).
- **Log Files.** NetShield can record the results of a scan in a virus incident log. See [View Logs](#).

Infected File Options

- **Move, Delete, or Ignore Infected Files.** NetShield can delete virus-infected files, move them to a "quarantine" directory, or ignore them until you decide what to do with them. See [Infected Action](#).
- **Virus Elimination.** Remove the virus itself with McAfee's [VirusScan](#).

You can select data by highlighting it. Use the mouse or the TAB key to make your selection(s).

Highlight a server and choose **Attach** to open it.

Highlight one or more volumes and choose **Start Scan** to begin scanning.

Choose **Stop Scan** to halt a scan in progress.

Select this check box to scan attached volumes when files are written to them.

Select this check box to scan attached volumes when they write to another server.

Select this radio button to disable periodic scanning.

Select this radio button to activate daily scanning.

Select this radio button to activate weekly scanning.

Select this radio button to activate monthly scanning.

Enter the start time of the scan in this field in twenty-four hour (xx:xx) format. For example, **06:00** would begin the scan at 6 a.m.; **18:00** would begin the scan at 6 p.m.

Select the desired start day from the provided list box.

Enter the date of the month you want the scan to begin by entering a numeral between 1 and 31.
For example, **1** begins the scan on the 1st of the month.

Select this check box if you want to notify one or more users upon virus detection.

Choose **Delete** to delete a user from the **Current User Contact List**.

Choose **Browse** to select from the directory or server tree.

Choose **OK** when you are finished with your selection(s) and want to return to the NetShield Console.

Choose **Cancel** to abort any changes and return to NetShield Console.

Choose **Set Password** to change your NetShield password for this server.

Choose **Help** for more information about this operation.

Choose **Load Profile** to load a previously saved configuration.

Choose **Save Profile** to save this configuration as a ***.dat** file.

Choose **Directory Tree/Server** to select another directory tree or another server.

Launching NetShield

When you first launch NetShield, you will be asked which server you want to [attach](#) to. Select the server you want by highlighting it and choosing **OK**. After entering your [NetShield Password](#), the [NetShield Configuration Window](#) for the server is displayed, with the [Scanning property page](#) active. You will also see the NetShield [Tool Bar](#) and [Menu](#).

Configure NetShield's [scanning](#), [notification](#) and [security](#) settings to your network's requirements. Save these settings in a configuration file so you can apply this protection to every server in your network (see [Save Configuration](#)).

To exit NetShield, select [Exit](#) from the **Tool Bar** or the **File** menu.

See also:

[How Do I...?](#)

[What is NetShield?](#)

[Updating NetShield](#)

[Configuring NetShield for Your Network](#)

Updating NetShield

New viruses - and new strains of older ones - are constantly appearing in and circulating throughout the computer community. McAfee updates the anti-virus data files regularly, usually monthly, but sooner if many new viruses have appeared. Each new version may detect as many as 60 to 100 new viruses.

To download McAfee updates, choose **About NetShield** from the **Help** menu, or refer to "Contacting McAfee" in your *Using NetShield* manual.

See also:

[Cross Server Updating](#)

[CRC Validation](#)

[NetLock Security](#)

Configuring NetShield for Your Network

McAfee recommends that you take a moment to examine NetShield's features and customize the settings to your network's needs, then save the settings in a configuration file (vir\$cfg.dat is the default). For more information about loading, viewing, and saving configurations, see [NetShield Configuration](#).

McAfee recommends the following:

NetShield can **delete, move, or ignore** an infected file. McAfee recommends that you move infected files to an administrator-access quarantine directory for later inspection. For more information, see [Infected Action](#).

NetShield can **notify selected users** and the **system console** of a possible infection. McAfee recommends that you enable these features so that system administrators are informed as soon as viruses are detected. For more information, see [Notification](#).

NetShield can record scan results in a **log file**. McAfee recommends that you enable this feature so that you can use the information to investigate any viral infections that arise, allowing you to track down their source and identify high-risk users or operations. For more information, refer to [Logging](#).

Some networks require even stricter security. NetShield can prevent write access to specific files, directories, or users, or can identify unknown viruses with [Cyclic Redundancy Checking](#). See [NetLock Security](#) for more information.

See also:

[How Do I...?](#)

[Updating NetShield](#)

[What is NetShield?](#)

If You Detect a Virus

McAfee strongly recommends that you get experienced help 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 or even destroy infected disks.

If you are at all unsure how to proceed once you have found a virus, contact McAfee for assistance. Refer **About NetShield** from the **Help** menu, or refer to “Contacting McAfee” in your *Using NetShield* manual.

See also:

[Infected Action](#)

[Notification Options](#)

[McAfee Support](#)

How Do I...?

Scanning questions

[How do I scan my network immediately?](#)

[How do I attach to another server?](#)

[How do I scan every day?](#)

[Can I scan every week? Every month?](#)

[How do I scan when files are copied to my network?](#)

[Can I scan outbound traffic too?](#)

[How can I reduce scanning time?](#)

[What does NetShield do when it finds a virus?](#)

[What should I do if NetShield finds a virus?](#)

Configuration questions

[How do I save a configuration?](#)

[How do I load a configuration?](#)

[What configuration should I use?](#)

Notification questions

[Who does NetShield tell when it finds a virus?](#)

[How do I create a log file of scanning events?](#)

[How do I alert users through a network broadcast message?](#)

[How about E-mail?](#)

[How do I set up pager notification?](#)

[My Notification choices don't appear on the Notification property page](#)

Security questions

[How do I use the Security menu?](#)

[Why doesn't my password work?](#)

[What is monitoring?](#)

[How do I restrict write access to specific directories?](#)

[How do I restrict write access to specific users?](#)

[How do I restrict write access by file or file type?](#)

[I'm still having trouble denying write access for files](#)

[What is CRC and how can I use it?](#)

[My Security choices don't appear on the Security property page](#)

For Help on Help, Press F1

See also:

[McAfee Support](#)
[What is NetShield?](#)

File Menu

The **File** menu allows you to load or save new scanning configurations, add servers to NetShield, or exit the program.

File
<u>O</u> pen...
<u>C</u> lose
<u>L</u> oad Configuration...
<u>S</u> ave configuration...
<u>E</u> xit

Choose [Open](#) to open a new **NetShield Configuration Window**.

Choose [Close](#) to close the active **NetShield Configuration Window**.

Choose [Load Configuration](#) to load a scanning configuration.

Choose [Save Configuration](#) to save a scanning configuration.

Choose [Exit](#) to terminate the NetShield session.

NOTE: Exiting the NetShield window does not unload the NetShield NLM from your server.

See also:

[Scan Menu](#)

[Notification Menu](#)

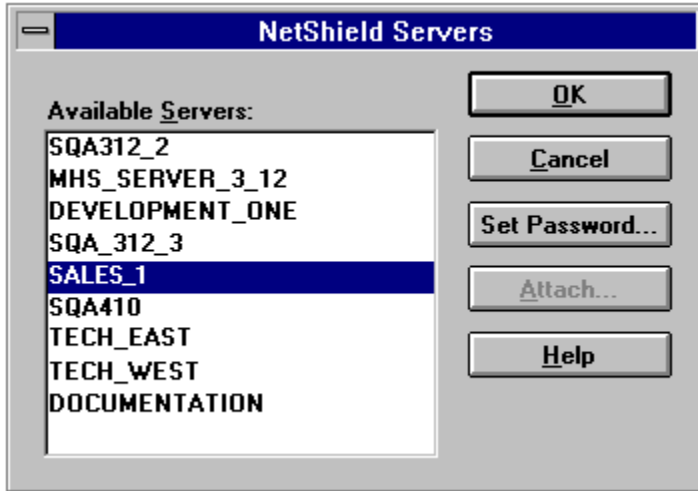
[Security Menu](#)

[View Menu](#)

[Window Menu](#)

Open

You can open another server by clicking once on the **Open** button from the [Tool Bar](#), or by choosing **Open** from the [File Menu](#).



Select a server and choose **OK** to add it to the **Available Servers** list. You will be prompted for your [NetShield Password](#). If you do not want to add a server, choose **Cancel** to return to the NetShield Configuration Window.

To change your [NetShield Password](#), select a server and choose **Password**. Enter your current password in the **Old Password** field, your new password in the **New Password** field, and confirm the new password by entering it in the **Retype New Password** field. Choose **OK** to change the password and attach to the selected server, or **Cancel** to abort changes.

See also:

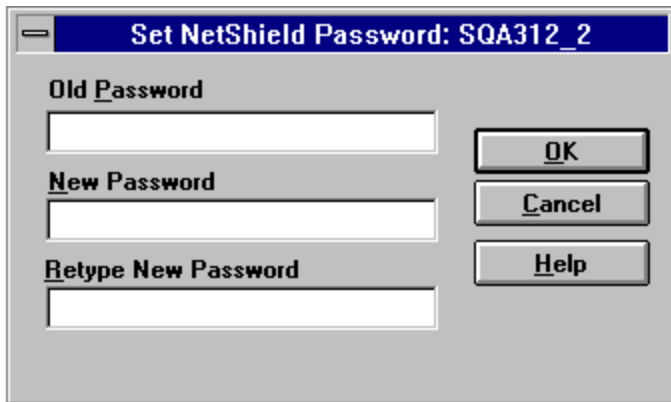
[Exclude Directories](#)
[NetShield Password](#)
[NetShield Configuration Window](#)
[Tool Bar](#)

NetShield Password

Each server can have its own NetShield password. The default password for all servers is `netshield`

NOTE: The password is not case-sensitive.

To change your NetShield password, [select a server](#) and choose **Set Password**. Enter the current password in the **Old Password** field, the new password in the **New Password** field, and the new password again in the **Retype New Password** field. Choose **OK** for NetShield to change the password and attach to the selected server, or **Cancel** to abort the changes.



The image shows a Windows-style dialog box titled "Set NetShield Password: SQA312_2". The dialog contains three text input fields stacked vertically, labeled "Old Password", "New Password", and "Retype New Password". To the right of these fields are three buttons: "OK", "Cancel", and "Help".

To attach to a server without changing the password, enter the password in the **Password** field and choose **OK**.

Enter your current password in this field.

Enter your new password in this field.

Confirm your new password by entering it again in this field.

Close

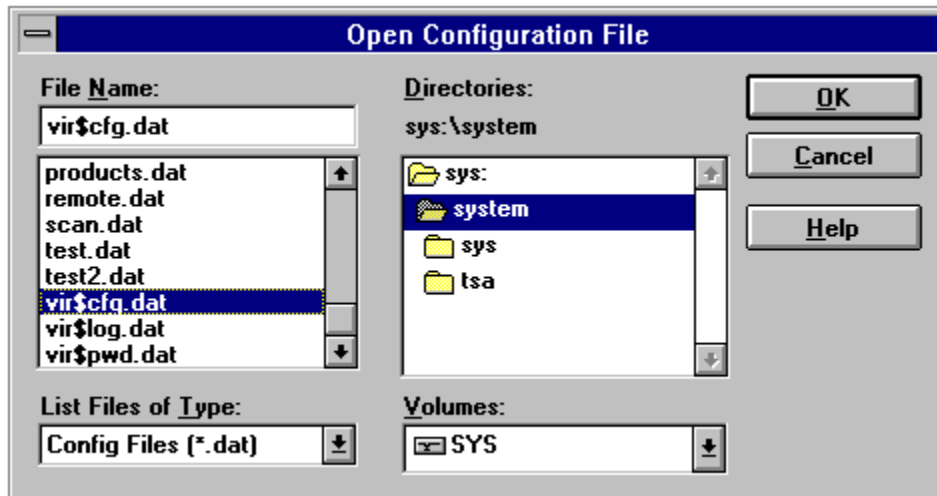
Choosing Close from the [File Menu](#) will close the active **NetShield Configuration Window**.

See also:

[NetShield Configuration Window](#)

Load Configuration

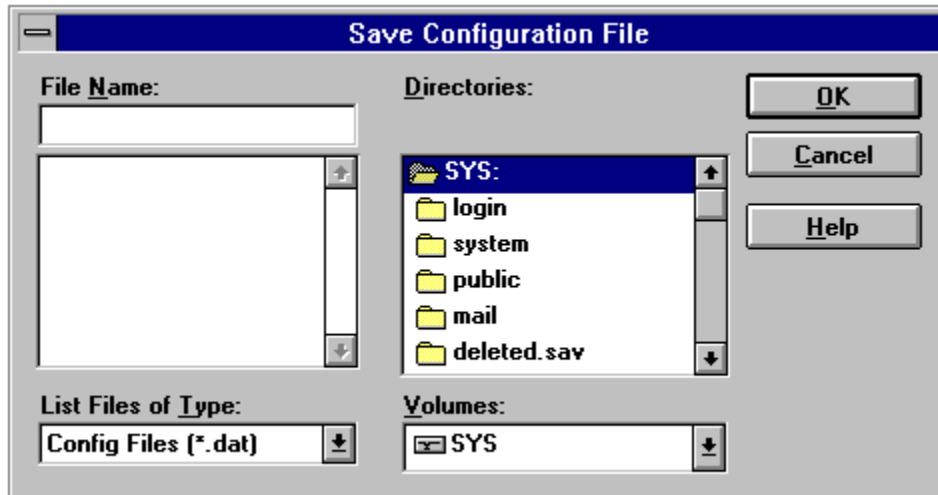
Choosing **Load Configuration** from the [File Menu](#) allows you to apply a previously saved configuration to the attached server.



Enter the name of the configuration file or select one from the list provided and choose **OK** to apply these settings to the attached server and return to the NetShield Configuration Window. Choose **Cancel** to abort any changes and return to the NetShield Configuration Window.

Save Configuration

Choosing **Save Configuration** from the [File Menu](#) allows you to save the current configuration in order to apply these settings to other servers.



Enter the name of the configuration file or select one from the list provided and choose **OK** to save these settings and return to the NetShield Configuration Window. Choose **Cancel** to abort any changes and return to the NetShield Configuration Window.

Scan

The **Scan** pull-down menu allows you to configure NetShield to meet your scanning needs.

Scan
<u>V</u> olume...
On <u>A</u> ccess...
<u>P</u> eriodic...
<u>C</u> RC Options...
<u>I</u> nfected Action...
<u>E</u> xclude Directories...
Cross <u>S</u> erver Updating...

Choose [Volume](#) to begin virus checking of one or more volumes on this server. (To choose another server, click on the [Open](#) button from the [Tool Bar](#) or select **Open** from the **File** menu.)

Choose [On Access](#) to configure NetShield to scan your network when inbound and/or outbound access is detected.

Choose [Periodic](#) to configure NetShield to scan your network on a daily, weekly, or monthly basis.

Choose [CRC Options](#) to configure NetShield's [CRC \(Cyclic Redundancy Check\)](#) settings.

Choose [Infected Action](#) to configure NetShield's response when a virus-infected file is detected.

Choose [Exclude Directories](#) to exclude low-risk directories from scans.

Choose [Cross Server Updating](#) to notify servers of new virus information.

See also:

[File Menu](#)

[Notification Menu](#)

[Security Menu](#)

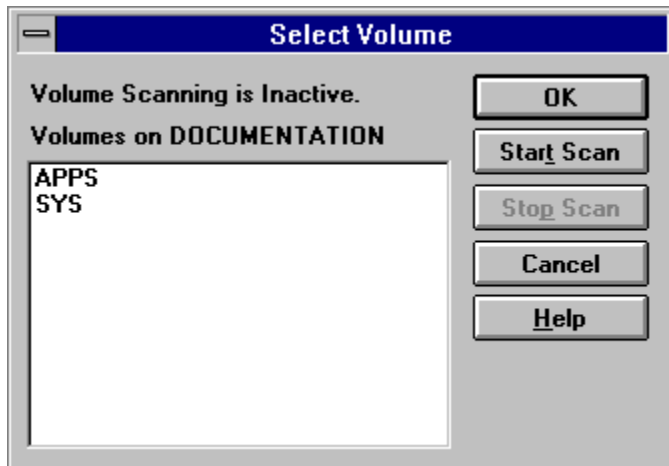
[View Menu](#)

[Window Menu](#)

CRC validation is a method for discovering unknown or new viruses. NetShield calculates a number based on the nature and size of the file, then periodically recalculates that number and compares it to the original number. If the CRC has changed, it is likely that the file is infected by an unknown virus. Because the CRC will change whenever a file is updated, it is recommended that CRC validation only be used in stable environments where few software updates are performed. Also, it is recommended that you do not perform CRC validation on data files, batch files, bindery files, or other files that are changed frequently.

On Demand Scanning

Scan attached volumes immediately by clicking once on the **On Demand Scanning** button from the [Tool Bar](#), or by choosing **Volume** from the **Scan** menu.



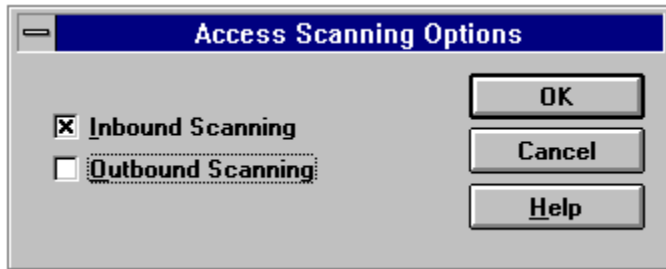
Select the volume(s) you want to scan by highlighting them, then choose **Start Scan**. Choose **Stop Scan** to halt any scan in progress. Choose **Cancel** to abort this menu.

See also:

- [How Do I...?](#)
- [Exclude Directories](#)
- [Exclude Files](#)
- [If You Detect a Virus](#)
- [Infected Action](#)
- [Notification Menu](#)
- [Scanning Options](#)
- [Select Server](#)

On Access Scanning

Configure NetShield's access scanning options by clicking once on the **On Access Scanning** button from the [Tool Bar](#), or by choosing **On Access** from the **Scan** menu.



NetShield will scan whenever executable files (.COM, .DLL, .EXE, .OVL, .SYS and .BIN) are written to and/or from the file server. You can edit this list of files through the File Server Console (refer to Chapter 7 of your *Using NetShield* manual).

Select the **Inbound Scanning** check box to scan attached volumes whenever these files are written to them. This will prevent virus-infected files from being copied to your network. Select the **Outbound Scanning** check box to scan attached volumes when these files are written to another server. This will prevent virus-infected files from being copied to another network.

See also:

[How Do I...?](#)
[If You Detect a Virus](#)
[Infected Action](#)
[Notification Menu](#)
[Scanning Options](#)

Periodic Scanning

Configure NetShield to automatically scan attached volumes by clicking once on the **Periodic Scanning** button from the [Tool Bar](#), or choosing **Periodic** from the **Scan** menu.

The screenshot shows a dialog box titled "Periodic Scanning Options". It has a blue title bar with a minus sign on the left. The dialog is divided into several sections:

- Frequency:** A group box containing four radio buttons: **Disable**, **Daily**, **Weekly**, and **Monthly**.
- When:** A group box containing three input fields: "Start time:" with the value "12:00", "Start day of week:" with a dropdown menu showing "Sunday", and "Start day of month:" with the value "0".
- Volumes to Scan:** A list box containing the text "APPS" and "SYS".
- Buttons:** A vertical stack of buttons on the right side: "OK", "Cancel", "Load Profile...", "Save Profile...", and "Help".

Select the desired Periodic Scanning option from the provided radio button:

[Daily Scanning](#)

[Weekly Scanning](#)

[Monthly Scanning](#)

To disable periodic scanning, select the **Disable** radio button.

See also:

[Load Profile](#)

[Save Profile](#)

[How Do I...?](#)

[If You Detect a Virus](#)

[Infected Action](#)

[Notification Menu](#)

[Scanning Options](#)

Daily Scanning

The image shows a dialog box titled "Periodic Scanning Options". It has several sections:

- Frequency:** Four radio buttons are present: "Disable", "Daily" (which is selected), "Weekly", and "Monthly".
- When:** Three input fields are shown:
 - "Start time:" with the value "0:01".
 - "Start day of week:" with a dropdown menu showing "Sunday".
 - "Start day of month:" with the value "0".
- Volumes to Scan:** A list box containing two items, "APPS" and "SYS", both of which are highlighted in blue.
- Buttons:** On the right side, there are five buttons: "OK", "Cancel", "Load Profile...", "Save Profile...", and "Help".

Select the **Daily Scanning** radio button for automatic scanning every day. Enter the start time in 24-hour format (xx:xx) in the **Start Time** field and select the volumes you want to scan by highlighting them.

In the above example, NetShield will scan the volumes APPS and SYS every morning at 12:01 a.m.

See also:

[Configure Periodic Scan](#)

Weekly Scanning

The image shows a dialog box titled "Periodic Scanning Options". It has a "Frequency" section with four radio buttons: "Disable", "Daily", "Weekly" (which is selected), and "Monthly". To the right of these are five buttons: "OK", "Cancel", "Load Profile...", "Save Profile...", and "Help". Below the frequency section is a "When" section with three fields: "Start time:" with the value "17:00", "Start day of week:" with a dropdown menu showing "Friday", and "Start day of month:" with the value "0". At the bottom is a "Volumes to Scan:" section with a list box containing "APPS" and "SYS", where "SYS" is highlighted.

Select the **Weekly Scanning** radio button for automatic scanning every week. Enter the time you want the scan to begin in 24-hour format (xx:xx) in the **Start Time** field; enter the day you want to scan in the **Start Day of Week** field; and select the volumes you want to scan by highlighting them.

In the above example, NetShield will scan the volume SYS every Friday at 5 p.m.

See also:

[Configure Periodic Scan](#)

Monthly Scanning

The screenshot shows a dialog box titled "Periodic Scanning Options". It has a "Frequency" section with four radio buttons: "Disable", "Daily", "Weekly", and "Monthly". The "Monthly" radio button is selected. To the right of these buttons are five buttons: "OK", "Cancel", "Load Profile...", "Save Profile...", and "Help". Below the frequency section is a "When" section with three fields: "Start time:" with the value "24:00", "Start day of week:" with the value "Friday", and "Start day of month:" with the value "1". At the bottom is a "Volumes to Scan:" section with a list box containing "APPS" and "SYS", both of which are highlighted in blue.

Select the **Monthly Scanning** radio button for automatic scanning every month. Enter the time you want the scan to begin in 24-hour format (xx:xx) in the **Start Time** field; enter the date you want to scan in the **Start Day of Month** field; and select the volumes you want to scan by highlighting them.

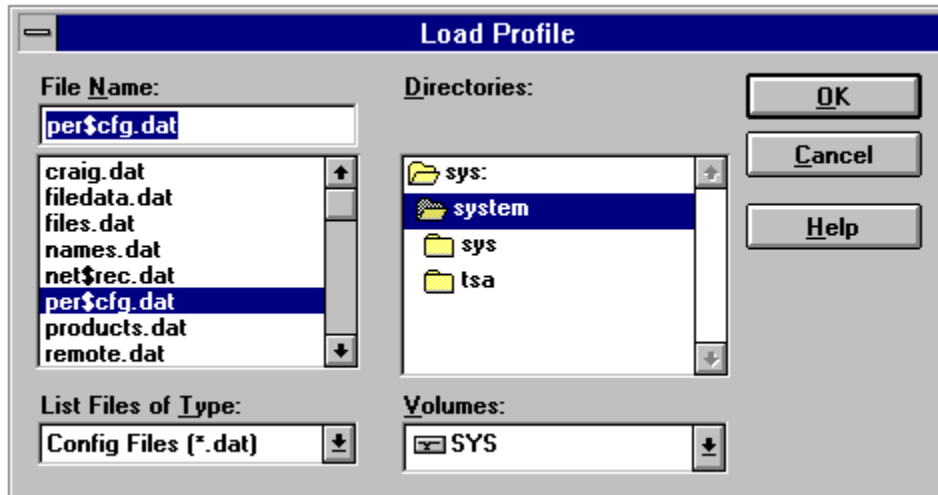
In the above example, NetShield will scan the volumes APPS and SYS at midnight on the 1st of every month.

See also:

[Configure Periodic Scan](#)

Load Profile

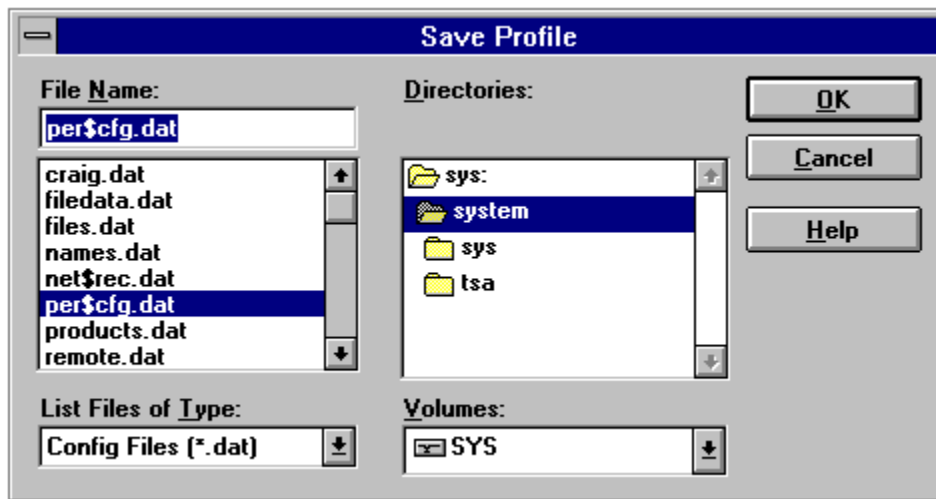
Choose **Load Profile** to apply a previously saved [Periodic Scanning Configuration](#) to the currently attached server.



Select a profile and choose **OK** to load these settings and return to the Configure Periodic Scan dialog box. Choose **Cancel** to abort this procedure and return to the Configure Periodic Scan dialog box.

Save Profile

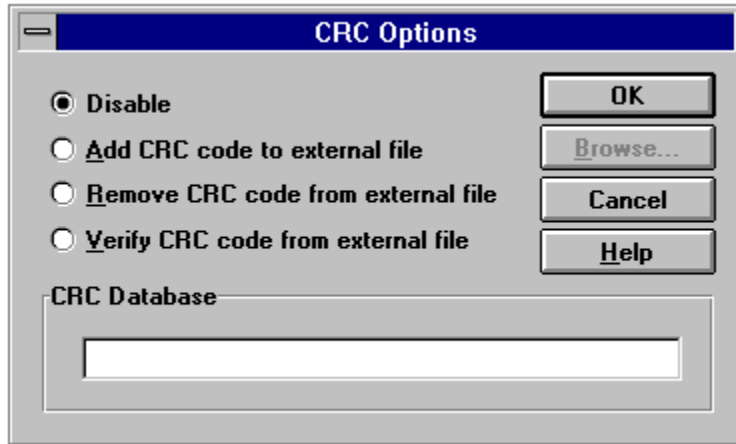
Choose **Save Profile** to save the [Periodic Scanning Configuration](#) in a configuration file.



Enter a file name for the profile and choose **OK** to save these settings and return to the Configure Periodic Scan dialog box. Choose **Cancel** to abort this procedure and return to the Configure Periodic Scan dialog box.

CRC Options

Configure NetShield's [CRC \(Cyclic Redundancy Check\)](#) options by selecting **CRC Options** from the [Scan](#) menu. This feature is recommended only for networks which are highly vulnerable to viruses, or which require additional security.



You can disable scanning files with CRC by choosing **Disable**. This is the recommended setting.

If you do choose to use CRC validation, perform the following procedure:

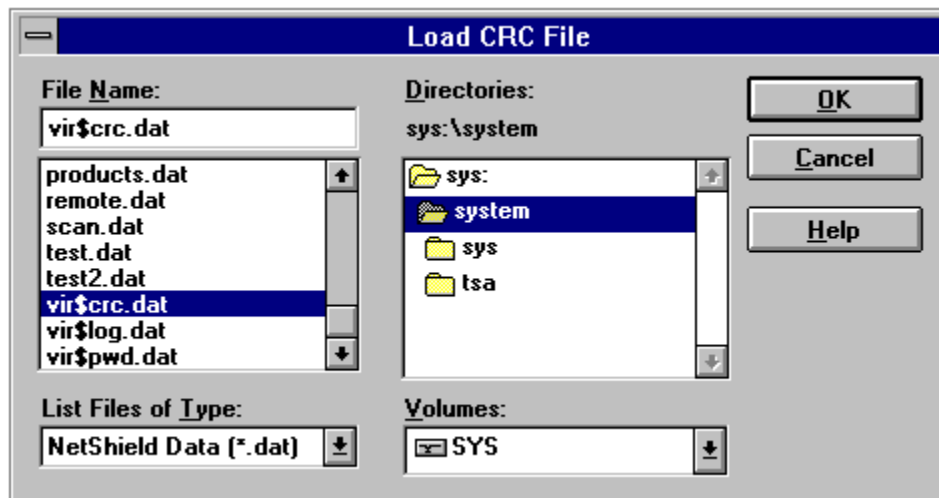
1. Choose **Add CRC code to external file** to save CRC codes to a database file during the next scan. After the next scan, the CRC codes will be saved to the database file, and you should disable this option.
2. Once the CRC codes have been saved to the database file, select **Verify CRC code from external file** to check for validation codes in subsequent scans. If NetShield determines that the current CRC codes have changed from the original codes (saved in the external database file), NetShield will warn you that the file may be infected by an unknown virus.
3. CRC validation requires on-going maintenance. Whenever you install new software or upgrade existing programs, you should delete the old CRC codes by choosing **Remove CRC code from external file**, then update the database by choosing **Add CRC code to external file**.

Choose [Browse](#) to search for a CRC database file.

See also:
[NetLock Security](#)

Load CRC File

You can search for a previously saved [CRC](#) database file by choosing **Browse** from the [CRC Options](#) window.



Enter the name of the CRC database file or select one from the list provided and choose **OK** to load this file and return to the CRC Options Window. Choose **Cancel** to abort any changes and return to the CRC Options Window.

Select this button to disable CRC validation.

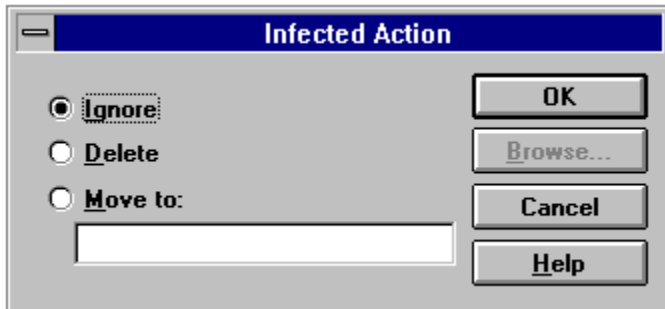
Select this button to set up a database file of CRC codes.

Select this button to begin CRC validation with the next scan.

Select this button to delete the database file of CRC codes.

Infected Action

Configure what action you want NetShield to take if a virus is detected by choosing **Infected Action** from the [Scan](#) menu.



NetShield can **Ignore** infected files found during a scan. Any infected files will be left 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.**

Infected files can be **Deleted** 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. The file is completely erased from your network and is not recoverable except from backups. This is the most secure option, but it can prevent you from recovering an infected file that you might want to save for further inspection.

NetShield can **Move** infected files to a quarantine directory where they can be subsequently inspected. To prevent users from inadvertently loading infected files into memory, be sure to set up a directory with administrator-only access. Select the directory you want to move infected files to with the **Browse** button.

See also:

[Configuring NetShield to Your Network](#)

[Exclude Directories](#)

[How Do I...?](#)

[If You Detect a Virus](#)

[Scanning Options](#)

[VirusScan](#)

Select this button to ignore infected files.

Warning: This option could lead to further viral infection. Be sure to check the scan log for infected files immediately after scanning.

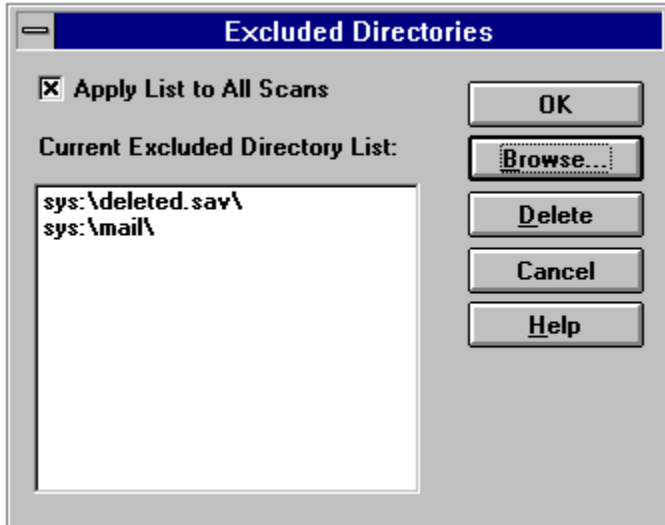
Select this button to delete and overwrite infected files. Files erased in this way cannot be recovered except from backups.

Select this button to move infected files to a quarantine directory.

Choose **Browse** to select the desired server or volume.

Exclude Directories

Exclude selected directories from scanning by choosing **Exclude Directories** from the [Scan](#) menu.



You may want to exclude directories which are unlikely to be infected by a virus to reduce scanning time. Typically, directories which contain only data files can be excluded from scans because most viruses attack only executable files. You can also ignore “quarantine” directories which contain virus-infected files.

Select the directories to be excluded by choosing **Browse**. Choose **Delete** to remove a directory from the list.

After you have selected the directories you want to be excluded, select the **Apply List to All Scans** check box. The listed directories will be ignored in subsequent scans. Clear this box in order to can the listed directories without removing them from the **Current Excluded Directory List**.

See also:

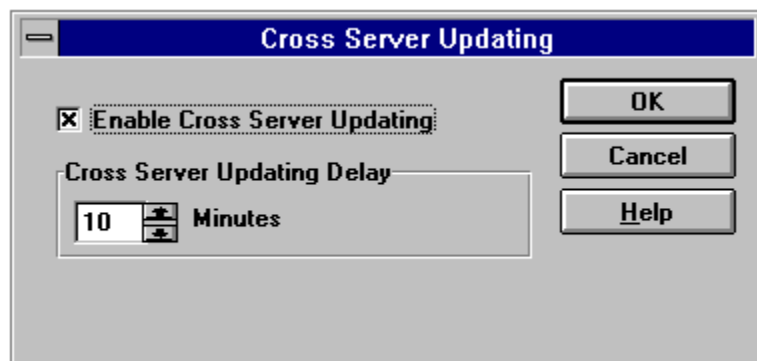
[Configuring NetShield for Your Network](#)
[Monitor For All Users](#)
[Scanning Options](#)

Choose **Delete** to remove a directory from the **Current Excluded Directory List**.

When this box is checked, the files in the listed directories (SYS:\deleted\sav\ and sys:\mail\) will be ignored during scans. Clear this box if you want to scan the excluded directories.

Cross Server Updating

Upgrade NetShield data files automatically across your network by choosing **Cross Server Updating** from the [Scan](#) menu.



McAfee releases updates of the NetShield data 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 this 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. Select **Enable Cross Server Updating** to enable this feature, or clear the box to disable it.

NetShield will check for updates based on the time interval set in the **Cross Server Updating Delay** field. Enter the time interval, in minutes (up to 25 minutes). For example, if you entered 10, NetShield would query other servers every ten minutes.

See also:
[Updating NetShield](#)

Select this box to enable **Cross Server Updating**.

Enter the time interval, in minutes (up to 25), that NetShield should check for updates.

Notification Menu

The **Notification** menu allows you to configure NetShield to alert selected users upon virus detection, using a broadcast message, pager message, E-mail message, or a console message. You can also set up a log file to keep track of scanning results.

Notification
<u>L</u> ogging...
<u>U</u> ser...
<u>M</u> ail...
<u>P</u> ager...
<u>C</u> onsole Messages

Choose [Logging](#) to enable logging and set up a log file.

Choose [User](#) to alert selected users by network broadcast if a virus is detected.

Choose [Mail](#) to alert selected users through E-mail.

Choose [Pager](#) to alert selected users by pager notification.

Choose [Console Messages](#) to enable console messages.

See also:

[File Menu](#)

[Scan Menu](#)

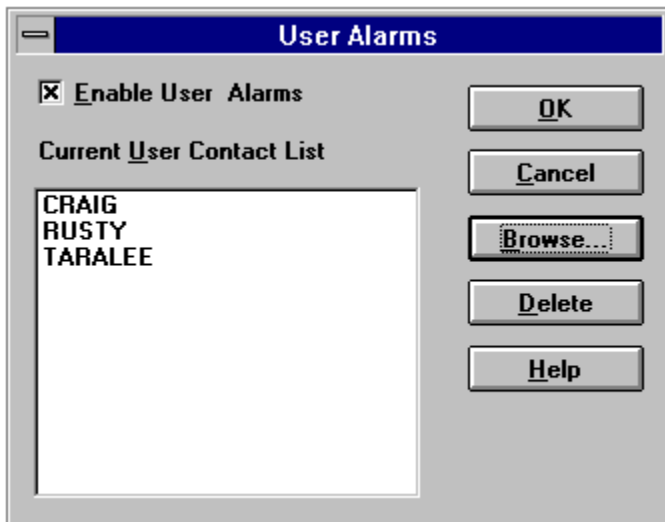
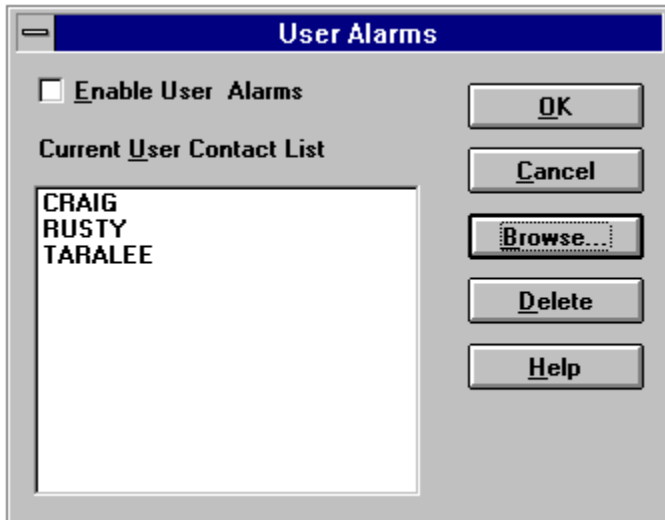
[Security Menu](#)

[View Menu](#)

[Window Menu](#)

Enabling Notification

Make sure that you have selected the **Enable Notification** check box for the type of notification you are attempting.

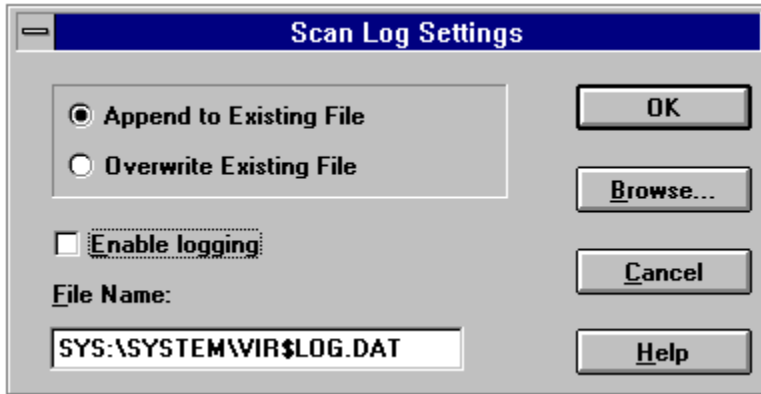


In the this example, users have been added to the Current User Contact List but they will not be notified because the **Enable User Messages** check box has not be selected.

These users will be notified because the **Enable User Messages** check box has been selected.

Logging

NetShield can record the results of scanning ([immediate](#), [periodic](#), or [access](#)) in a log file that you can later use to investigate problems. NetShield records the date and time of the scan and, if any viruses were detected, an entry for each file suspected to contain a virus (file name, location, and virus name).



To enable logging, choose **Logging** from the [Notification](#) menu. Enter the path and a file name to save the log file as (or use the [Browse](#) button) and select the **Enable Logging** check box.

Choose **Overwrite** to write over the old log file, or **Append** if you want to save new logging information at the end of an existing log file.

See also:

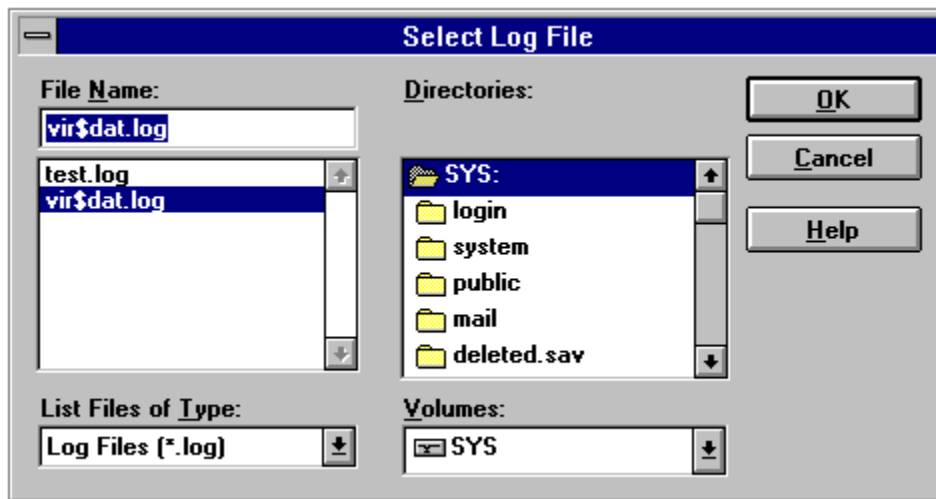
[Configuring NetShield for Your Network](#)

[How Do I...?](#)

[View Logs](#)

Select Log File

Choose **Browse** from the [Scan Log Settings](#) dialog box to search for a log file



Choose **OK** to select the highlighted file and return to the previous window. Choose **Cancel** to abort any changes and return to the previous window.

Select this button to save new information at the end of an existing log file.

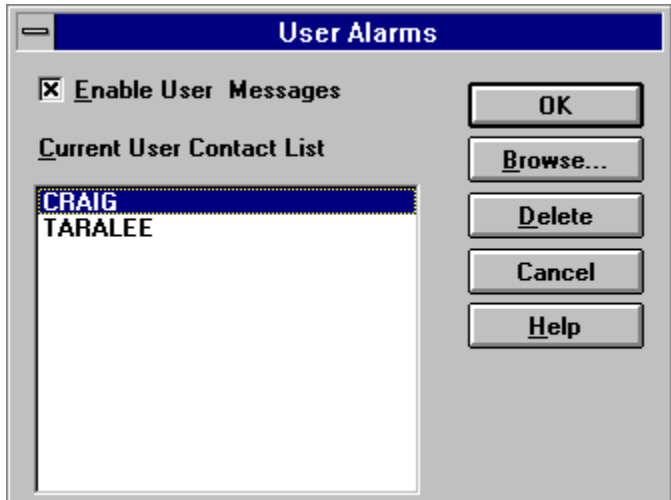
Select this button to overwrite an existing log file.

Select this check box to enable logging.

Enter the directory path and the log file name (**vir\$log.dat** is the default) in this field.

User Notification

Select the user(s) you want to be alerted when NetShield detects a virus by clicking once on the **Configure User Alerts** button, or by choosing **User** from the **Notification** menu.



Add one or more users to the **Current User Contact List** by choosing [Browse](#). Select the **Enable User Notification** check box to notify these users when a virus is detected.

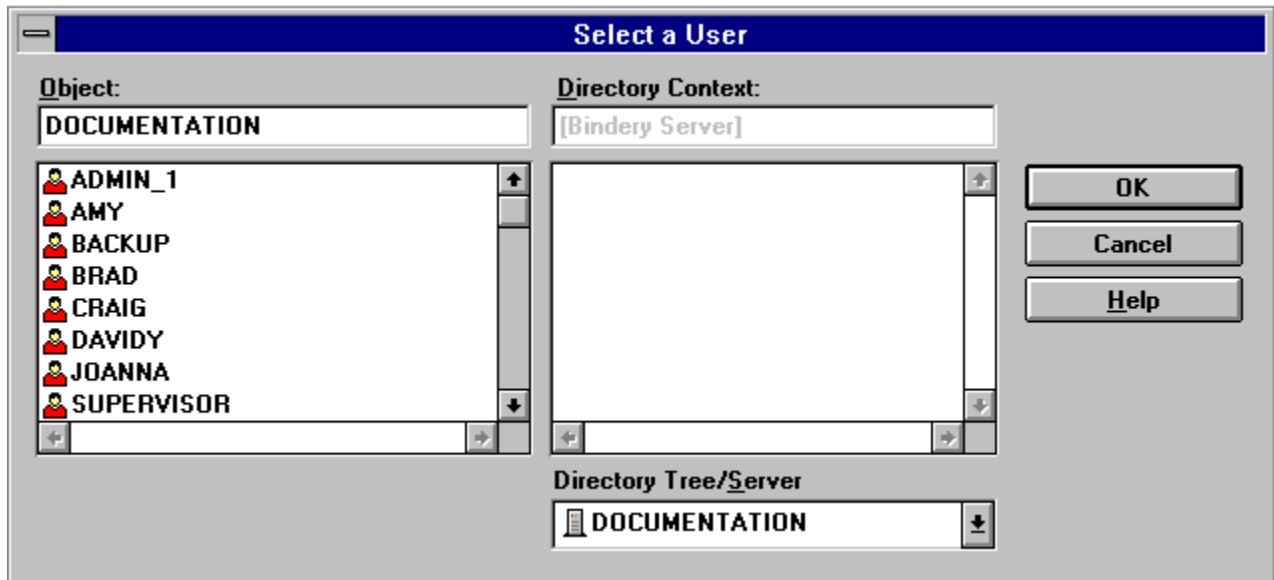
See also:

[How Do I...?](#)

[Notification Options](#)

Select a User

Add a user to the list by choosing **Browse**.



Enter the name of the user or select one from the list provided and choose **OK** to add this user to the list and return to the previous window. Choose **Cancel** to abort any changes and return to the previous window.

NOTE: Directory trees are only displayed if you are logged in as an NDS (NetWare Directory Services) user.

See also:
[Configure User Alerts](#)

Highlight one or more users to be notified and choose OK to add them to the **Current User Contact List**.

These users will **not** be notified if NetShield detects an infected file. To add a user to the notification list, highlight him or her and choose **OK**.

Mail Notification

Alert selected users to a detected virus through E-mail with the **Mail** command, in the [Notification](#) menu.



NOTE: NetShield uses Novell's Message Handling Service (MHS) to direct E-mail messages throughout your network. You must have Novell Basic or Global MHS installed and running on your network in order to use this feature.

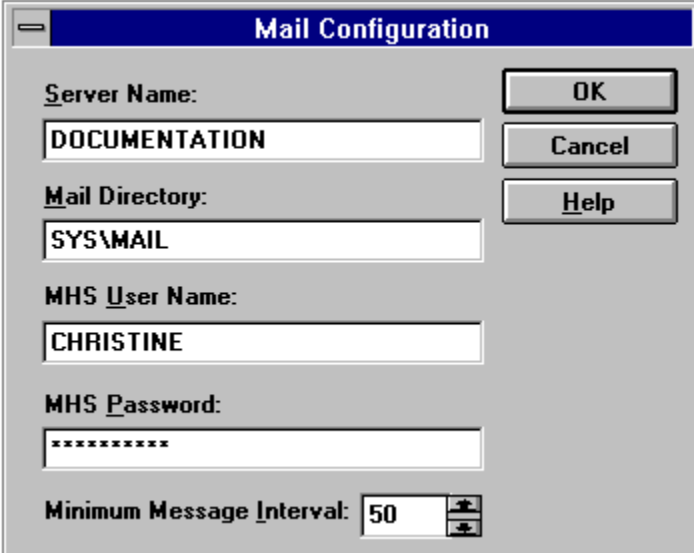
If a virus is detected during scanning, NetShield will send an E-mail notification to selected users when the scan is concluded. (If you are using [On Access Scanning](#), NetShield will send a notification immediately. You can delay notification until scanning is complete by setting a **Minimum Message Interval**, using the [Settings](#) button.)

Select the **Enable Mail Messages** check box to activate this feature. Configure NetShield to your network's GMHS system using the [Settings](#) button. Use the [Add](#) and **Remove** to edit the **Current Mail Recipient List**.

See also:
[How Do I...?](#)
[Notification Options](#)

Mail Settings

Configure NetShield's [Mail Notification](#) to your network using the **Settings** button.



The image shows a 'Mail Configuration' dialog box with the following fields and controls:

- Server Name:** DOCUMENTATION
- Mail Directory:** SYS\MAIL
- MHS User Name:** CHRISTINE
- MHS Password:** *****
- Minimum Message Interval:** 50 (with up/down arrows)
- Buttons:** OK, Cancel, Help

Enter the location of GMHS (Novell's Message Handling Service) by entering the **MHS Server Name, Mail Directory, User Name** and **Password**.

If you are using [On Access Scanning](#), NetShield will send an immediate notification for each infected file detected. In order to prevent a backlog of redundant messages, you can set a **Minimum Message Interval**, in minutes, that NetShield should wait before sending a new notification, allowing NetShield to continue scanning and sending one consolidated E-mail notification instead of a rapid succession of messages.

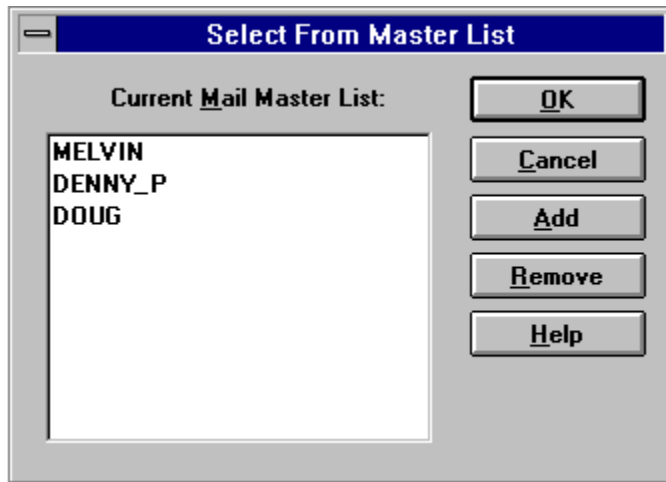
See also:

[How Do I...?](#)

[Notification Options](#)

Select From Master List

Add a user to the list by choosing **Browse** from the [Mail Notification](#) dialog box.



Highlight the user(s) you want to add to the list and choose **OK** to add the user(s) to the list and return to the previous window. Choose **Cancel** to abort any changes and return to the previous window.

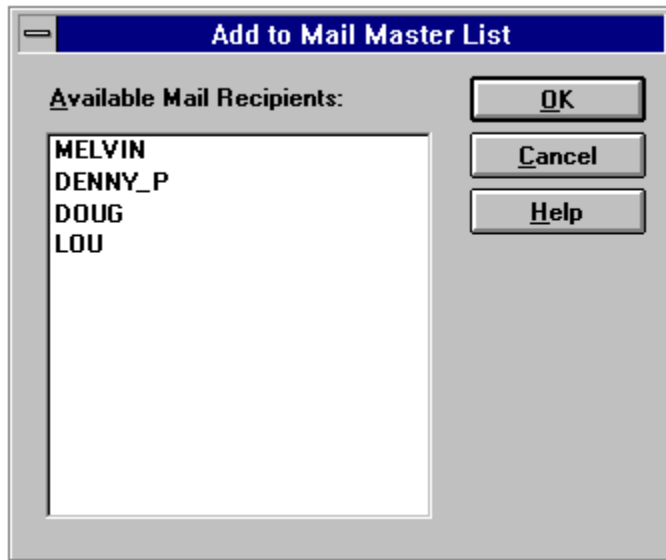
Choose [Add](#) to add additional users to the master list. Highlight a user and choose **Remove** to delete the user from the notification list.

Add a user to the list by choosing **Add**.

Remove a user from the list by choosing **Remove**.

Add to Master List

Add additional users to the master list by choosing **Add** from the [Select From Master List](#) dialog box.



Highlight the user(s) you want to add to the master list and choose **OK** to add the user(s) to the master list and return to the previous window. Choose **Cancel** to abort any changes and return to the previous window.

If the users you want to add are not listed, you may have your [GMHS Settings](#) configured incorrectly.

Enter the name of the Novell GMHS server in this text box.

Enter the GMHS Mail Directory in this text box.

Enter the user name for Novell's Message Handling Service.

Enter the password for Novell's Message Handling Service.

Enter the Minimum Message Interval, in minutes, to delay repeated messages.

Select this box to enable mail messages.

Edit the **Current Mail Recipient List** using the **Add** and **Remove** buttons.

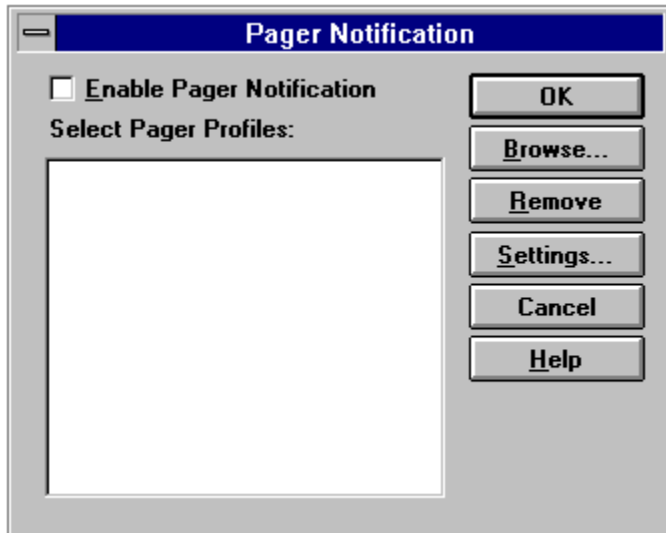
Add a recipient using this button.

Remove a recipient using this button.

Use the **Settings** button to configure NetShield.

Pager Notification

NetShield can notify users about a detected virus through a pager. Choose **Pager** from the [Notification](#) menu.



NOTE: You must have a Hayes-compatible modem installed, running, and accessible on your NetShield server to use this feature.

NOTE: Pager Notification is not supported on SFT III systems.

NOTE: AIOCOMX.NLM and AIO.NLM must be loaded in order to use pager notification on NetWare 3.X and 4.X servers.

If a virus is detected during scanning, NetShield will page selected users when the scan is concluded. (If you are using [On Access Scanning](#), NetShield will send a page immediately. You can delay paging until scanning is complete by setting a **Minimum Message Interval**, using the **Settings** button.)

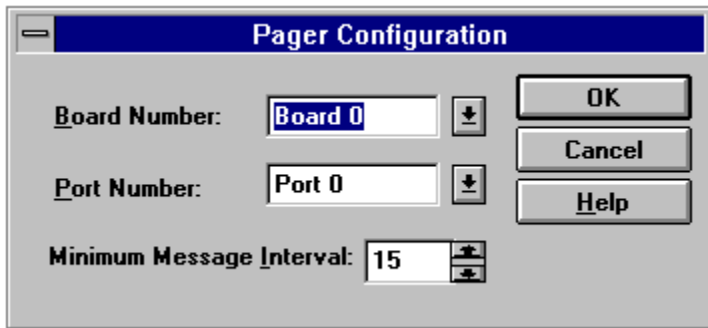
Select the **Enable Pager Notification** check box to activate this feature. Configure NetShield to your server's Hayes-compatible modem using the [Settings](#) button. Remove a user from the **Selected Pager Profiles** list by choosing **Remove**. Add a user to the **Selected Pager Profiles** list by choosing [Browse](#).

See also:

[How Do I...?](#)
[Notification Options](#)

Pager Settings

Configure NetShield's [Pager Notification](#) to your network using the **Settings** button.



The image shows a dialog box titled "Pager Configuration". It contains three input fields and three buttons. The "Board Number" field is set to "Board 0", the "Port Number" field is set to "Port 0", and the "Minimum Message Interval" field is set to "15". The buttons are "OK", "Cancel", and "Help".

Enter the following information about your Hayes-compatible modem, which must be installed on your NetShield server: **Communications Board Number**, as defined by the AIOCOMX.NLM utility, which determines the board number of the modem; and **Port Number**, as defined by the AIOCOMX.NLM utility, which determines the port number of the modem.

If you are using [On Access Scanning](#), NetShield will send an immediate page for each infected file detected. In order to prevent a backlog of redundant messages, you can set a **Minimum Message Interval**, in minutes, that NetShield should wait before sending a new page, allowing NetShield to continue scanning and sending one page instead of a rapid succession of pages.

See also:

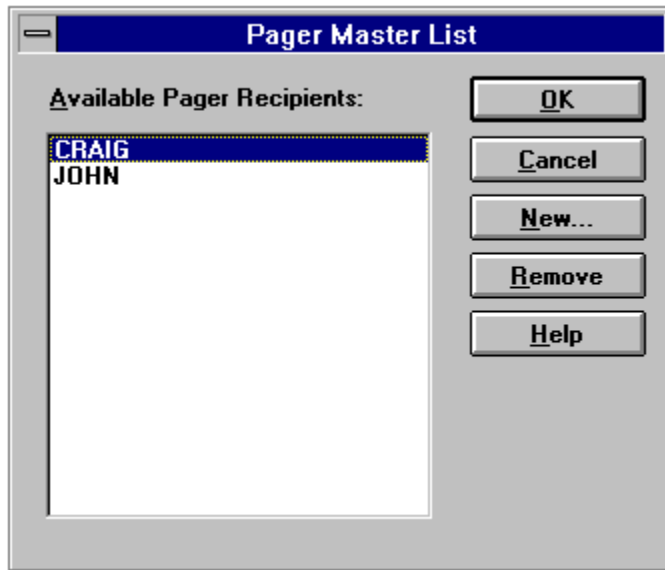
[How Do I...?](#)

[Notification Options](#)

[Pager Messages](#)

Pager Master List

Add a user to the list by choosing **Browse** from the [Pager Notification](#) dialog box.



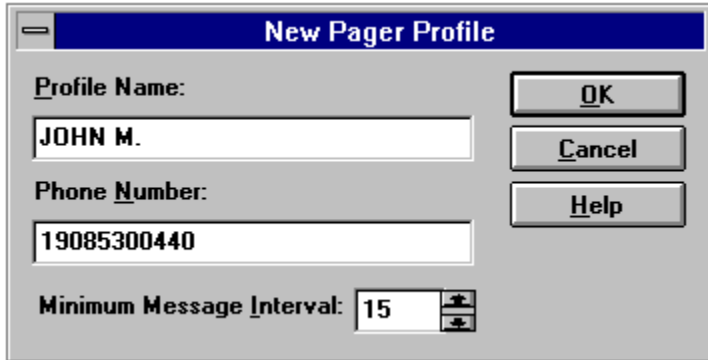
Highlight the user(s) you want to add to the list and choose **OK** to add the user(s) to the list and return to the previous window. Choose **Cancel** to abort any changes and return to the previous window.

Choose [New](#) to add additional users to the master list. Highlight a user and choose **Remove** to delete the user from the notification list.

Choose **New** to add a new pager to the master list.

New Pager Profile

Add additional users to the master list by choosing **New** from the [Pager Master List](#) dialog box.



The image shows a dialog box titled "New Pager Profile". It has three input fields on the left and three buttons on the right. The "Profile Name" field contains "JOHN M.". The "Phone Number" field contains "19085300440". The "Minimum Message Interval" field is a spin control with the value "15". The buttons are labeled "OK", "Cancel", and "Help".

Enter the new pager's **Profile Name** and **Profile Number** in the fields provided. Use the spin controls to set the **Minimum Message Interval**, in minutes, to prevent redundant pager messages if several infected files are found in rapid succession.

Console Messages

NetShield can display messages about infected files on the NetShield Console. This can provide an alternative to notifying network administrators without using network broadcasts or E-mail messages.

To enable Console Messages, choose **Console Messages** from the [Notification](#) menu. When Console Messages are active, a check mark will appear in the **Notification** pull-down menu and the message "Console Messages are active" will appear in the **Infection Notification** box of the [Notification property page](#).

See also:

[How Do I...?](#)

[Notification Options](#)

Enter the communications board number of the server's Hayes-compatible modem.

Enter the port number of the server's Hayes-compatible modem.

Select this check box to enable pager notification.

Edit the **Selected Pager Profiles** list using the **Browse** and **Remove** buttons.

Add a recipient using the **Browse** button.

Security Menu

The **Security** menu offers high-level security for your network. NetShield can prevent users from writing executable files to your network, prevent write access to sensitive directories, or even suspend write access for specific users.

The **Security** menu is password protected to ensure that only authorized users have access. The default password is

login admin

NOTE: The password is not case-sensitive.

It is recommended that the default password is changed the first time NetShield is run. The NetLock password can only be changed from the server running the NetShield NLM.

NOTE: You must activate NetLock security by selecting **Enable NetLock Security** from the [Security Settings](#) menu.



Choose [Security Password](#) to enable the Security menu.

Choose [Security Settings](#) to activate Security settings, load or save a security configuration, or record unauthorized write attempts to a log file.

Choose [Edit Master List](#) to create a list of files or file types to monitor.

Choose [Select From Master List](#) to monitor these files or file types.

Choose [Exclude Files](#) to allow access for frequently updated files.

Choose [Monitor For All Users](#) to monitor write access to sensitive directories.

Choose [Monitored Users](#) to limit access to specific users.

Choose [Temporary Authorization](#) to grant temporary administrator access.

See also:

[Cyclic Redundancy Checking](#)

[Monitoring](#)

[NetLock Password](#)

[File Menu](#)

[Scan Menu](#)

[Notification Menu](#)

View Menu
Window Menu

Launch NetLock

Launch NetLock by clicking once on the **Launch NetLock** button from the [Tool Bar](#), or by choosing **Security Password** from the **Security** menu.

You will be asked to enter your [NetLock Password](#). The default password is

`login admin`

The NetLock password can only be changed from the server running the NetShield NLM.

See also:

[NetLock Password](#)

[Security Menu](#)

Password

NetShield uses two passwords: a NetShield password, which is used in attaching to servers (refer to [NetShield Password](#)), and a NetLock password, which is used to enable the [Security Menu](#).

The default password for the NetShield password is `netshield`

The default password for the NetLock password is `login admin`

NOTE: The passwords are not case-sensitive.

The NetShield password can be changed by entering a new password in the New Password field when you are attaching to another server. The NetLock password can only be changed from the server running the NetShield NLM.

Security Settings

The Security Settings menu allows you activate NetShield's security options, load or save security configuration files, and to record unauthorized write attempts in a log file.



Select the **Enable NetLock Security** check box to activate your security configuration. **If this check box is not selected, your security options will not be enforced.**

If you are using [Monitoring](#), you can record unauthorized write attempts to a log file by entering a log file name in the **Log Access to File** field.

Save the security configuration choices you have made by selecting **Save**. You can load a previously saved security configuration file by choosing **Load**. Search for a configuration file by choosing **Browse**.

Select this check box to activate your security choices. If this check box is not selected, your security options will not be enforced.

Enter the filename of the security log file in this field.

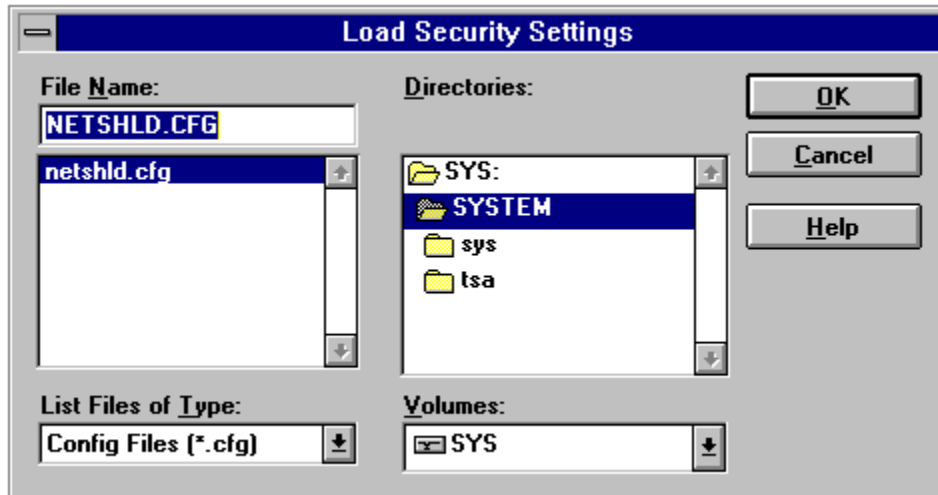
Choose **Save** to save your security configuration.

Choose **Load** to load a previously saved security configuration.

Choose **Browse** to search for a previously saved security configuration.

Security Settings File Management

You can load or save security settings to quickly apply your NetLock security choices to other servers in your network.



Choose **Save** to save the configuration file. Enter the file name or select one from the list box provided.

Choose **Load** to load a configuration file. Enter the file name or select one from the list box provided.

Choose **Browse** to search for a Security log file. (See [Monitoring](#))

Monitoring

With the NetLock security options, you can monitor write access to specific files, file types, directories, or users. NetShield can both prevent write access and log unauthorized attempts, keeping suspicious files off of your network. You can exclude specific files or file types from monitoring (such as data files or backup files). NetShield also allows you to temporarily suspend read-only access by granting Temporary Authorization to a specific user to allow for software installations or upgrades.

To monitor specific files or file types, see [Edit Master List](#)

To monitor specific directories, see [Monitor For All Users](#)

To monitor specific users, see [Monitored Users](#)

To log unauthorized write attempts, see [Security Settings](#)

To exclude specific files or file types from monitoring, see [Exclude Files](#)

To grant temporary authorization to a user, see [Temporary Authorization](#)

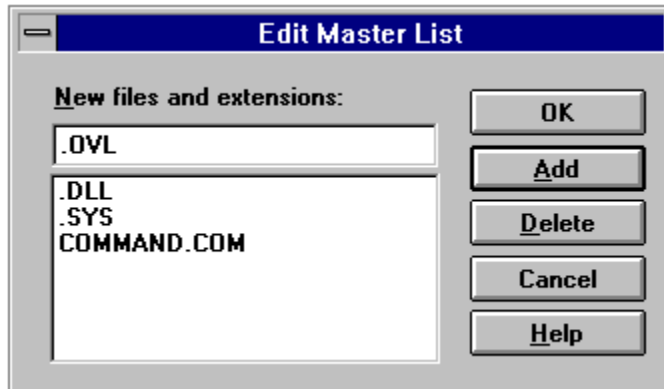
See also:

[How Do I...?](#)

[Security Menu](#)

Edit Master List

Choose **Edit Master List** from the [Security](#) menu to create or maintain a master list of files and file extensions to monitor for write access. For example, you might want to monitor unauthorized attempts to write executable files to your network. Viruses are often concealed in executable files, and by watching activity on those files you can learn more about possible infections.



Typically, you will want to monitor unauthorized write attempts of standard executable files (EXE, COM, SYS, BIN, OVL, and DLL).

To add an extension to the master list, enter a period and the extension (up to three letters). To add a file to the master list, enter the full file name including the period and the extension. Choose **Add** to monitor this file or extensions for unauthorized activity.

Highlight a file or extension and choose **Delete** to remove the file or extension from the Master List.

NOTE: If you want to monitor these files, you will have to add them to **the Entries From Master List**. See [Select From Master List](#).

See also:

[Select From Master List](#)

[Monitoring](#)

[Monitor For All Users](#)

[Security Menu](#)

Monitor a file or extension by highlighting it on the Master List and choosing **Add**.

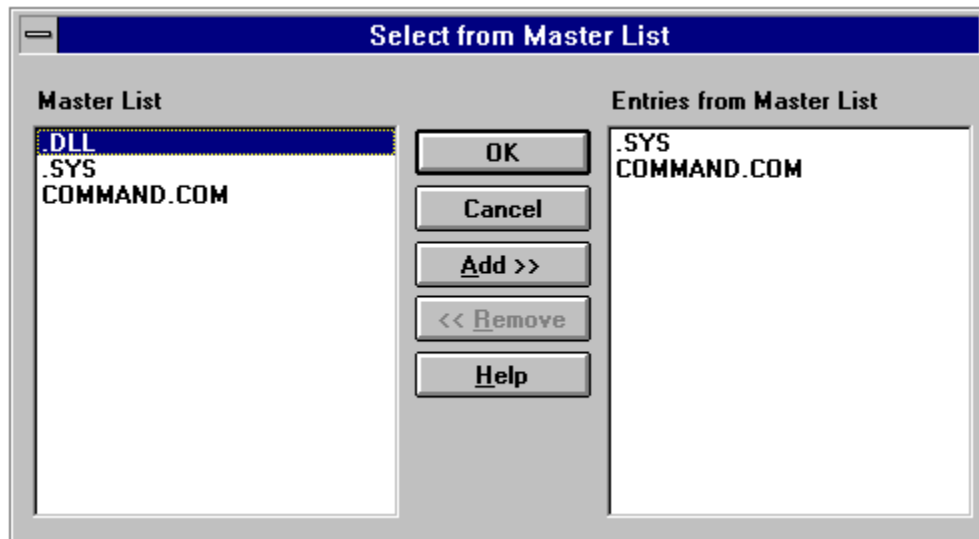
Remove a file or extension from the Master List by highlighting it and choosing **Delete**.

Add a file or extension to the Master List by entering the file name or extension in the provided text box.

Select From Master List

Once you have created your [master list](#), you can select the files or extensions you want NetShield to monitor by choosing **Select From Master List** from the [Security Menu](#).

NOTE: Files or file types in the master list will only be monitored if they are in the Entries From Master List window (on the right side of the screen).



(To add a file or extension to the Master List, choose [Edit Master List](#) from the [Security Menu](#).)

Add a file or extension to be monitored by highlighting the file or extension in the **Master List** window and choosing **Add**. Stop monitoring a file or extension by highlighting the file or extension in the **Entries From Master List** window and choosing **Remove**.

Removing a file or extension from the **Entries From Master List** does not delete it from the **Master List**.

See also:
[Edit Master List](#)
[Monitoring](#)
[Security Menu](#)

To monitor a file or extension, highlight it and choose **Add**.

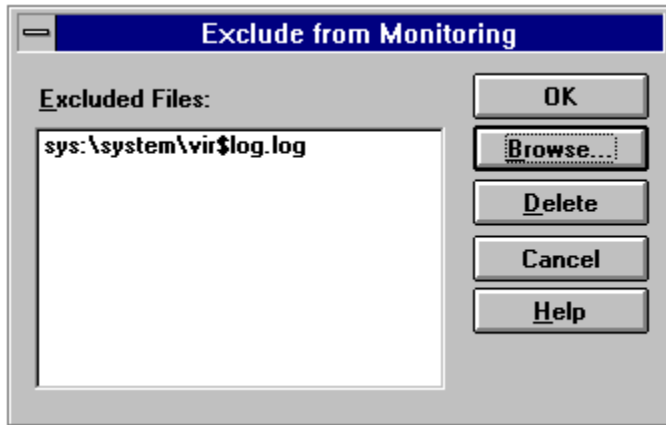
To stop monitoring a file or extension, highlight it and choose **Remove**.

These files are being monitored.

This file is not being monitored.

Exclude Files

You can exclude certain files or extensions from monitoring for write access by choosing **Exclude Files** from the [Security Menu](#).



You might want to exclude certain files, such as a frequently updated backup file, from monitoring. In the above example, NetShield will allow write access to its own log file.

Choose **Browse** to add a file or extension to the **Exclude Files** list. Choose **Delete** to remove a file or extension from the **Exclude Files** list.

See also:

[Monitoring](#)

[Edit Master List](#)

[Exclude Directories](#)

[Select From Master List](#)

[Security Menu](#)

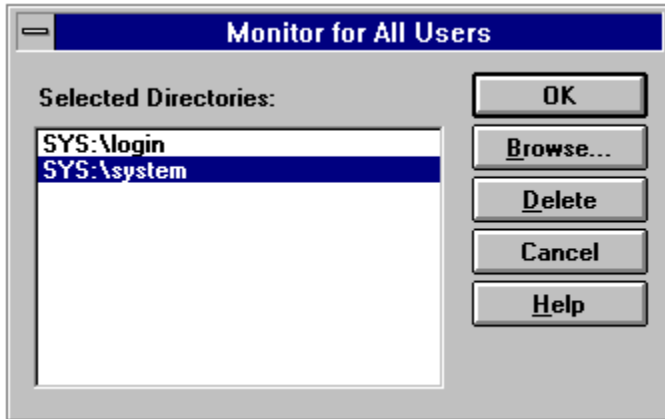
Add a file to the **Excluded Files** list by choosing **Browse**.

Remove a file from the **Excluded Files** list by choosing **Delete**.

NetShield will allow access to this file.

Monitor For All Users

Select directories that NetShield should watch for unauthorized write attempts by selecting **Monitor For All Users** from the [Security Menu](#). For example, you might want to monitor directories that contain application executables.



Choose [Browse](#) to add a directory to the **Selected Directories** list. Choose **Delete** to remove a file or extension from the **Selected Directories** list.

See also:

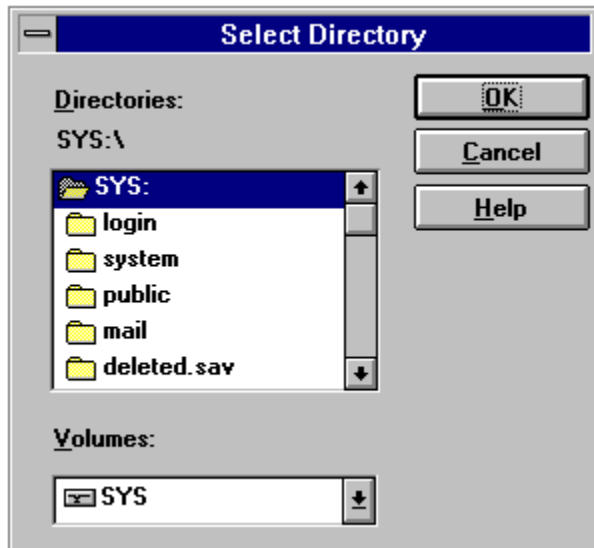
[Monitoring](#)

[Exclude Directories](#)

[Security Menu](#)

Select Directory

Choose **Browse** to search for a directory.



Choose **OK** to select the highlighted directory and return to the previous window. Choose **Cancel** to abort any changes and return to the previous window.

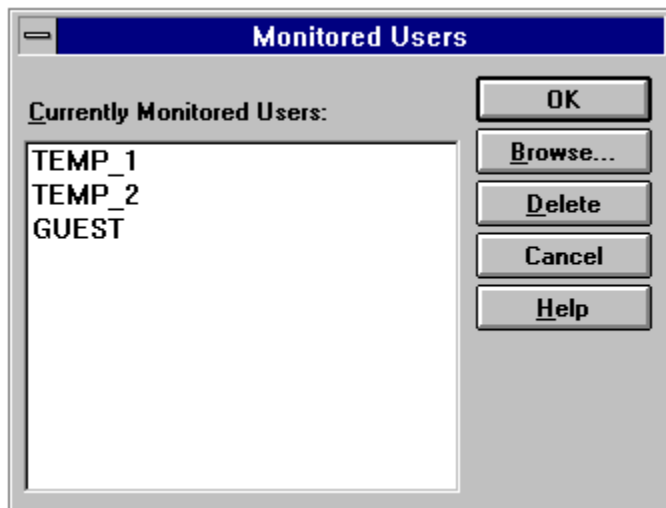
Add a file to the Selected Directories list by choosing **Browse**.

Remove a file from the Selected Directories list by choosing **Delete**.

NetShield will deny write access to these directories.

Monitored Users

You may want to restrict certain users from write attempts to all volumes and directories. Choose **Monitored Users** from the [Security Menu](#).



To add a user to the Monitored Users list, choose [Browse](#). To remove a user from the Monitored User list, choose **Delete**.

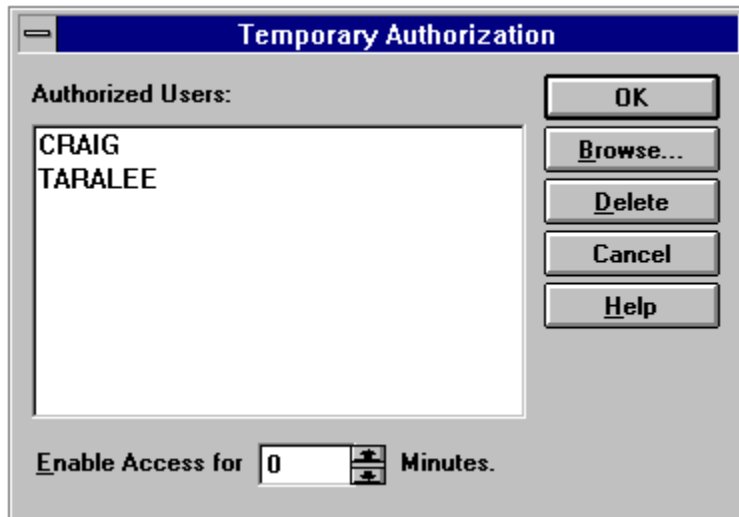
See also:

[Monitoring](#)
[Security Menu](#)

Monitored users are restricted from write access to protected servers. They can only write files which are being [excluded from monitoring](#). Edit the Monitored Users list by using the **Browse** and **Delete** buttons.

Temporary Authorization

You can suspend read-only protection on monitored directories so that authorized users can make changes. Choose **Temporary Authorization** from the [Security Menu](#).



To add a user to the **Temporary Authorization** list, choose **Browse**. To remove a user from this list, choose **Delete**.

To enable access, you must enter a number in the **Enable Access For** field. This number is the time, in minutes, that the temporary user(s) will have to make any changes in the protected directories. NetShield will display 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** as the default access time.

See also:

[Monitoring](#)
[Security Menu](#)

Edit the **Authorized Users List** using the **Browse** and **Delete** buttons.

Remove a user using the **Delete** button.

View Logs

View NetShield's *.log files by clicking once on the **View Logs** button.

The screenshot shows a dialog box titled "Periodic Scanning Options". It has a standard Windows-style title bar. The dialog is divided into three main sections. The first section, "Frequency", contains four radio button options: "Disable", "Daily" (which is selected), "Weekly", and "Monthly". The second section, "When", contains three input fields: "Start time:" with the value "0:01", "Start day of week:" with a dropdown menu showing "Sunday", and "Start day of month:" with the value "0". The third section, "Volumes to Scan:", contains a list box with two items, "APPS" and "SYS", both of which are highlighted in blue. To the right of the "Frequency" section are five buttons: "OK", "Cancel", "Load Profile...", "Save Profile...", and "Help".

The log files contain scanning results. These files can be useful in tracking down the source of viral infections. To enable logging, choose [Logging](#) from the [Notification Menu](#).

See also:

[Logging](#)

NetShield Configuration Files

Save or load scanning configuration by choosing [Load Configuration](#) or [Save Configuration](#) from the [File Menu](#).

The screenshot shows a dialog box titled "Periodic Scanning Options". It has a blue header bar with the title. Below the header, there are several sections:

- Frequency:** A group box containing four radio buttons: "Disable", "Daily" (which is selected), "Weekly", and "Monthly".
- When:** A group box containing three input fields: "Start time:" with the value "0:01", "Start day of week:" with a dropdown menu showing "Sunday", and "Start day of month:" with the value "0".
- Volumes to Scan:** A list box containing two entries, "APPS" and "SYS", with "APPS" selected.

On the right side of the dialog, there are five buttons: "OK", "Cancel", "Load Profile...", "Save Profile...", and "Help".

NetShield's configuration files can be viewed as Microsoft Write files by choosing **Configuration File** from the [View Menu](#). Select the file (with a .RPT extension) you wish to view and choose **OK**. The file can be converted into Microsoft Write text by choosing **Convert**.

You can save a configuration as a configuration report file (with a .RPT extension) through the File Server Console. Refer to "Configuration File Management" in Chapter 7, "The File Server Console" of your *Using NetShield* manual.

See also:

[Configuring NetShield for Your Network](#)

VirusScan

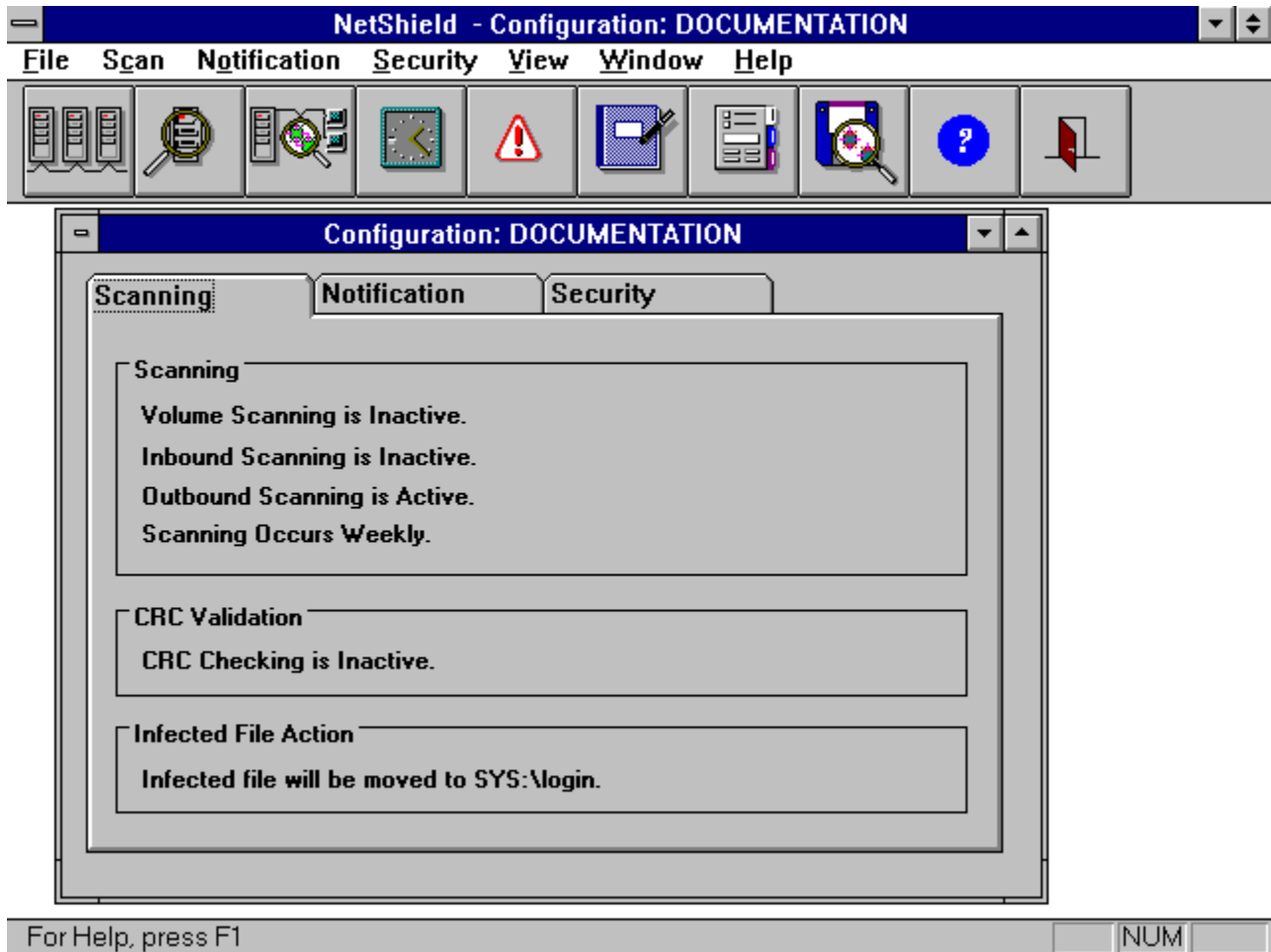
Launch the VirusScan module by clicking once on the **VirusScan** button. (Product sold separately.)

See also:

[If You Detect a Virus
Infected Action](#)

NetShield Configuration Window

The NetShield Configuration Window is used to monitor your current NetShield configuration.



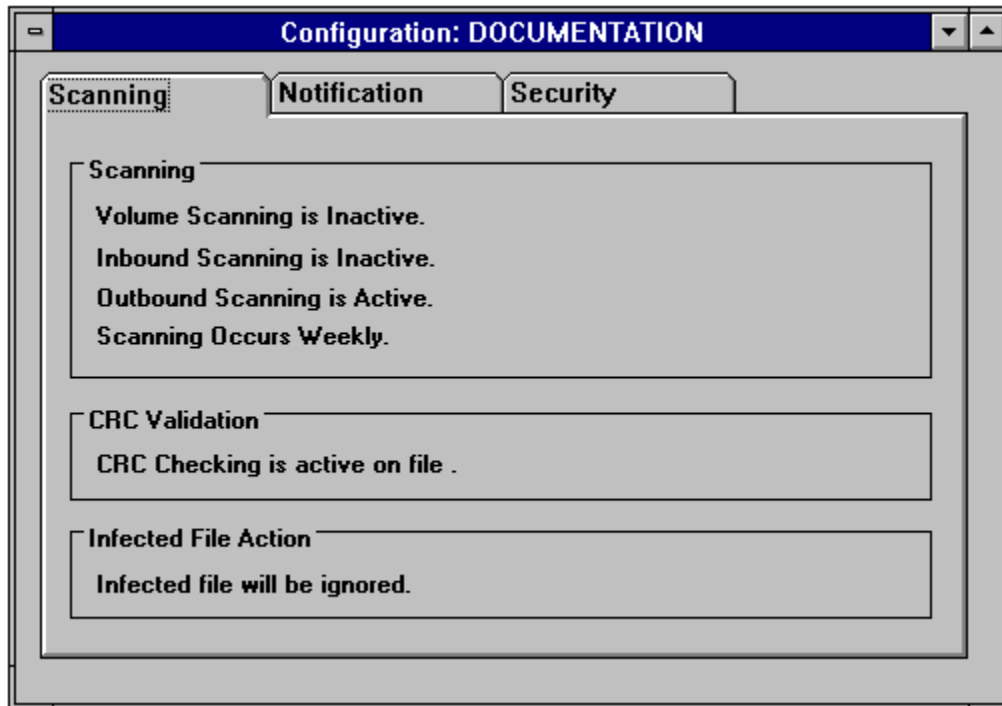
The NetShield Configuration Window contains three property pages: [Scanning](#), [Notification](#), and [Security](#).

To open a new NetShield Configuration Window, choose **Open** from the [File](#) menu. To close the NetShield Configuration Window, choose **Close** from the [File](#) menu.

See also:
[Window Menu](#)

Scanning Property Page

The Scanning property page displays NetShield's current scanning configuration.



See also:

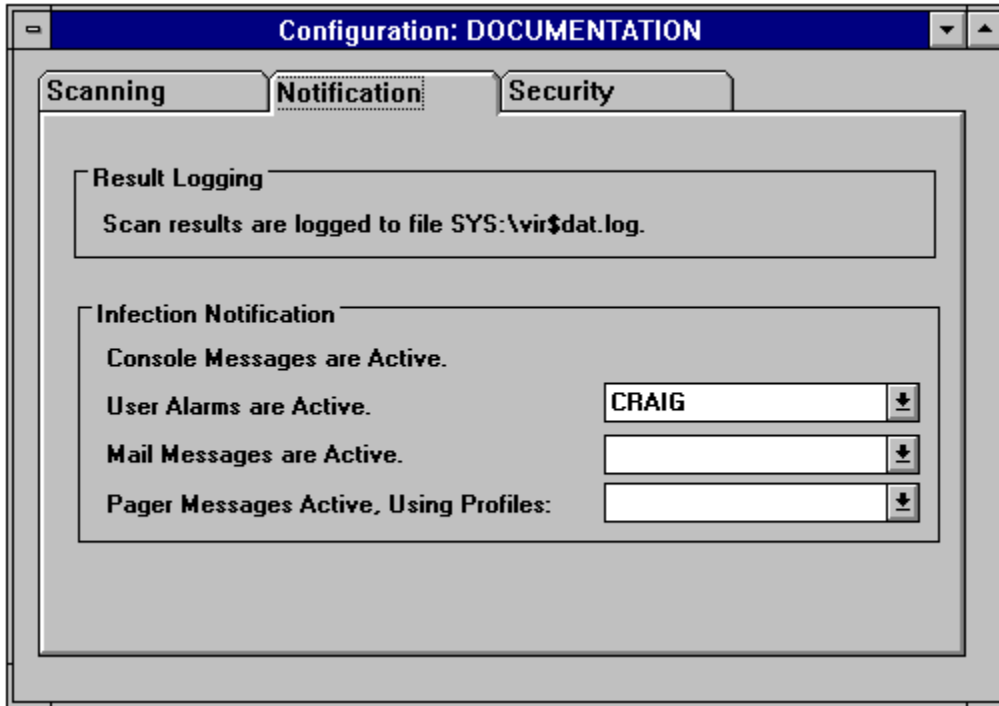
[How Do I...?](#)

[NetShield Configuration Window](#)

[Scanning Options](#)

Notification Property Page

The Notification property page displays NetShield's current notification configuration.



See also:

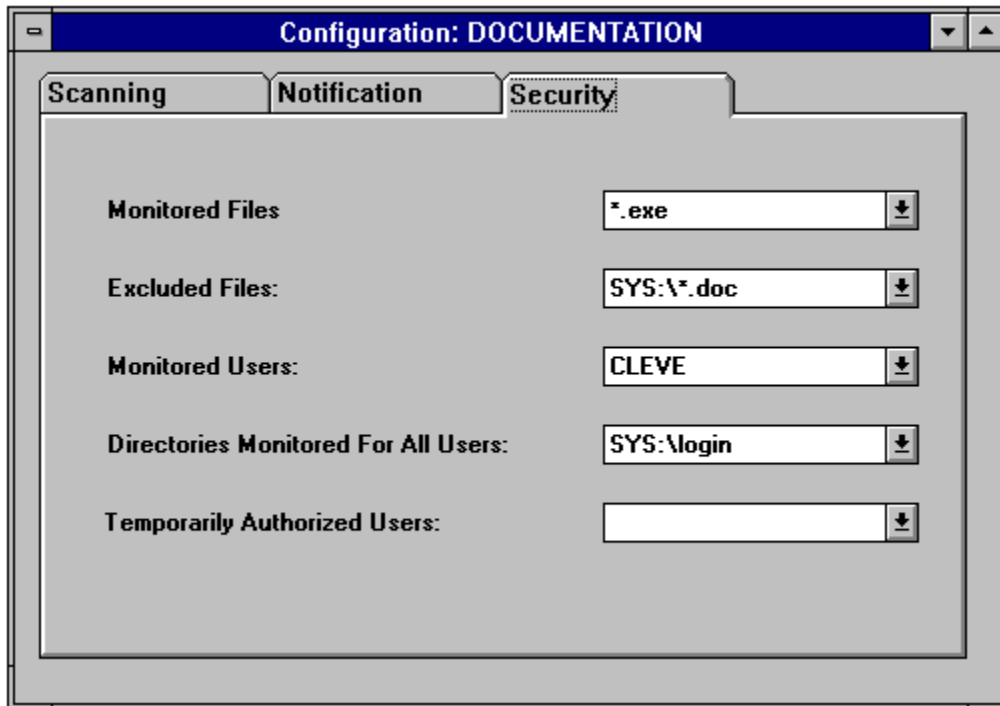
[How Do I...?](#)

[NetShield Configuration Window](#)

[Notification Options](#)

Security Property Page

The Security property page displays NetShield's current security configuration.



See also:

[How Do I...?](#)

[NetShield Configuration Window](#)

[Security Options](#)

[Monitoring](#)

This message indicates if there is an on-going scan.

Inbound scanning monitors files being written to your network.

Outbound scanning monitors files being written from your network.

Periodic scanning can occur on a daily, weekly, or monthly basis.

CRC checking is a powerful tool for detecting unknown or new viruses.

Infected files can be ignored, deleted, or moved to a quarantine directory.

NetShield can record scanning results in a log file.

Network administrators can be notified of a detected virus by an alert message on the NetShield server.

Alert specific users using a network broadcast message.

Alert specific users using Novell's GMHS to send E-mail.

Alert specific users by paging them using a Hayes-compatible modem.

Monitor specific files or types of files for possible infection.

Ignore files high traffic files, such as back-up files that are frequently updated.

Monitor specific users to prevent unauthorized access.

Monitor write access to specific directories.

Grant temporary administrator access for software upgrades or installs.

Tool Bar



Click on the Tool Bar button you would like to know more about.

You can show or hide the Tool Bar by choosing **Tool Bar** from the **View** menu.

Status Bar

The Status Bar provides information about the current operation.

You can show or hide the Status Bar by choosing **Status Bar** from the **View** menu.

Open

Click once on this button to select another server.

On Demand Scanning

Click once on this button to begin scanning attached volumes immediately.

On Access Scanning

Click once on this button to configure NetShield to scan automatically on inbound and/or outbound access.

Periodic Scanning

Click once on this button to configure NetShield to scan automatically on a daily, weekly, or monthly basis.

User Notification

Click once on this button to configure NetShield to notify users if upon virus detection.

View Log Files

Click once on this button to view NetShield ***.log** files.

View Configuration Files

Click once on this button to view NetShield ***.rpt** files.

VirusScan

Click once on this button to launch the VirusScan module. (Product sold separately).

Help

Click once on this button to launch NetShield help.

Exit

Click once on this button to end your NetShield session.

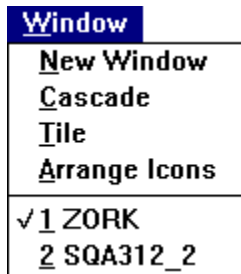
Menu

NetShield's pull-down menus allow you configure your network's scanning, security, and notification options.

File Scan Notification Security View Window Help

Window Menu

The Window menu allows you to switch between attached servers, or to arrange icons on the NetShield Console.



See also:

- [File Menu](#)
- [Scan Menu](#)
- [Notification Menu](#)
- [Security Menu](#)
- [View Menu](#)

Select **New Window** to create a copy of the active NetShield Configuration window.

Select **Cascade** to view attached servers in cascade format.

Select **Tile** to view attached servers in tile format.

Select **Arrange Icons** to arrange minimized configuration windows.

Switch between NetShield Configuration windows of attached servers.

View Menu

Choose **View | Tool Bar** to hide/show the NetShield tool bar. Choose **View | Status Bar** to hide/show the NetShield status bar.

View
<u>L</u> og File...
<u>C</u> onfiguration File...
✓ <u>T</u> oolbar
✓ <u>S</u> tatus Bar

View NetShield's configuration report files as Microsoft Write files by selecting [View Configuration](#). View NetShield's log files by selecting [View Logs](#).

See also:

[File Menu](#)
[Scan Menu](#)
[Notification Menu](#)
[Security Menu](#)
[Window Menu](#)

Hide or show the NetShield [Tool Bar](#) by selecting **View | Tool Bar**. A check mark indicates that the Tool Bar is shown.

Hide or show the NetShield [Status Bar](#) by selecting **View | Status Bar**. A check mark indicates that the Status Bar is being shown.

Help

Launch this Help system by clicking once on the **Help** button or by selecting **Index** or **Search** from the **Help** menu.

If you need help on Help, press F1.

See also:

[How Do I...?](#)

[Configuring NetShield for Your Network](#)

[If You Detect a Virus](#)

Exit

End your NetShield session by clicking once on the Exit button, or by choosing Exit from the File menu.

On demand scanning allows you to examine your network at any time. You can interrupt scans using the **Stop Scan** command.

On access scanning will prevent users from copying infected files to and/or from your network, depending on the configuration you choose.

Periodic scanning allows you to perform automatic scans during periods of low network traffic, providing network protection without sacrificing network performance.

For highly secure networks, NetShield can restrict specific users to read-only access, monitor access to read-only directories or specific file types, or grant temporary administrator access to facilitate software upgrades or installations.

Infected files can quickly spread through an unmonitored network. These files can be ignored for future inspection or deleted and overwritten so they cannot be recovered except from backups. We recommend that you move the files to a secure directory so that they can be evaluated later, or even uploaded to McAfee for expert inspection. For more information, see [McAfee Support](#) or refer to Chapter 1, "Introduction," of your *Using NetShield* manual.

McAfee's VirusScan and VShield™ (products sold separately) can be used to eliminate the virus from your network. For more information, see [McAfee Support](#) or refer to Chapter 1, "Introduction," of your *Using NetShield* manual.

We recommend that you alert system administrators as soon as a virus is detected using console messages and/or a network broadcast message to specific users. Networks using Novell's Message Handling Service can send E-mail to your users. If you have a Hayes-compatible modem available to the server running NetShield, you can alert users through pager messages.

NetShield can record any virus incidents in a log file, providing an important tool for investigating any viral infections on your network. You can view or print this log file for future reference.

McAfee Support

For help in using this product, we invite you to contact McAfee Associates technical support. You can contact us at:

McAfee, Inc.

2710 Walsh Avenue
Santa Clara, CA 95051-0963
USA

Phone: (408) 988-3832

FAX: (408) 970-9727

Hours: 6 a.m. to 5 p.m. PST

McAfee BBS: (408) 988-4004
1200 bps to 28,800 bps
8 bits, no parity, 1 stop bit
24 hours, 365 days a year

CompuServe: GO MCAFEE

Internet: support@mcafee.com

America Online: MCAFEE

Password

Enter your NetShield password in the text field provided.



A screenshot of a Windows-style dialog box titled "NetShield Password: SALES_1". The dialog box has a grey background and a blue title bar. On the left side, there is a label "Password" above an empty text input field. On the right side, there are three buttons stacked vertically: "OK", "Cancel", and "Help". Each button has a small icon on the left and text on the right.

The default password for NetShield is `netshield`.

NOTE: The password is not case-sensitive.

