What is a computer virus?

A software program which attaches itself to another program on a disk or lurks in a computer's memory and spreads from one program to another.

In addition to self-replication, viruses have the capability to damage data, cause computers to crash, and display offending or bothersome messages.

{button ,JI(`SHIELD.HLP',`Boot_virus')} Boot virus
{button ,JI(`SHIELD.HLP',`File_virus')} File virus
{button ,JI(`SHIELD.HLP',`Stealth_virus')} Stealth virus
{button ,JI(`SHIELD.HLP',`Multi_partite_virus')} Multi-partite virus
{button ,JI(`SHIELD.HLP',`Mutating_virus')} Mutating virus
{button ,JI(`SHIELD.HLP',`Encrypted_virus')} Encrypted virus
{button ,JI(`SHIELD.HLP',`Polymorphic_virus')} Polymorphic virus

{button ,KL(`Why do I need to scan for viruses?',0,`',`')} Related Topics

What is a boot virus?

A boot virus copies itself from the boot sector of one drive to another (eg: floppy drive to hard drive).

What is a file virus?

A file virus attaches itself to a program. Whenever the program runs, the virus attaches itself to other programs.

What is a stealth virus?

A stealth virus hides itself to evade detection. It stealth virus may be a boot virus or a file virus.

What is a multi-partite virus?

A multi-partite acts like a boot virus and a file virus by spreading through boot sectors and files.

What is a mutating virus?

Mutating viruses change their shape to avoid detection. Many mutating viruses are also encrypted viruses.

What is an encrypted virus?

Encrypted viruses encrypt part of their code to avoid detection. Many encrypted viruses are also mutating viruses.

What is a polymorphic virus?

Polymorphic viruses are similar to mutating viruses. Upon each instance of copying itself, it slightly changes its code to avoid detection.

Why do I need to scan for viruses?

In today's environment, safe computing practices are no longer a luxury - they are a necessity.

Computer viruses no longer attack your computing environment exclusively. They attack all computing environments you are in contact with through diskettes, networks, modems, and even the Word file you gave to a coworker to edit.

Consider the value of the data on your computer. It is probably irreplaceable or would require a significant amount of time and money to replace. Consider the value of the data on all of the computers you contact, the computers those computers contact, and so on.

Viruses are non-discriminatory. They may damaging something as simple as your high score on Solitaire, or something as important as the novel you spent years writing.

McAfee's virus scanning solutions should top the list of your safe computing practices. Scheduled periodic scans of your computer offers added assurance you are practicing safe computing.

{button ,AL(`Major features and benefits of NetShield NT;What is a computer virus?',0,`',`')} Related Topics

Major features of NetShield NT

Superior detection

- Consistently detects over 96% of the more than 6500 known viruses
- NCSA certified
- Uses patented Code Trace and Code Matrix technology to accurately pinpoint known generic and unknown boot, file, multi-partite, stealth, mutating, polymorphic and encrypted viruses.

Automated protection

- Native NT Services and Devices - supports Windows NT services and file system.
- Real-time scanning of file all accesses with minimal resource utilization.
- Flexible scheduling and immediate scanning options.
- Advanced alerting features including Alphanumeric Pager, Trouble Ticket, e-mail via
- SMTP and the NT event logging features.

Administrative ease

- Scan Wizard assists users in creating new scan tasks.
- AutoUpdate features allows for immediate or scheduled updating via a central shared location or FTP download.
- Enhanced virus encyclopedia enables users to learn more about various virus types.

About McAfee

Founded in 1989, McAfee Inc. is the leading provider of productive computing tools for DOS, OS/2, UNIX, and Windows environments. Our anti-virus products are used by more than 16,000 corporations worldwide. Our utility products provide data security, automated version updating, and system inspection and editing. McAfee is also the pioneer and leading provider of electronically distributed software. All of McAfee's products may be purchased through dealers or downloaded from bulletin board systems and on-line services around the world.

McAfee does not stop at developing the world's best anti-virus and utility products. We back them with the industry's best service and technical support. Product support is provided by a full-time staff of virus researchers, programmers, and support professionals; and delivered directly by McAfee or our network of more than 150 authorized agent offices in 50+ countries worldwide.

McAfee NetShield Server software

NetShield for Windows NT is a client-server application with the NetShield Server software composing the server end of the relationship. Once configured by the Console, the Server software runs in the background without any assistance.

McAfee NetShield Console

NetShield for Windows NT is a client-server application with the NetShield Console composing the client end of the relationship. The Console controls and configures the Server software and may run on the server or any attached workstation.

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

To start the Console, locate its icon and double-click.

What are tasks?

Tasks are individually configured jobs which are responsible for virus protection activities. Each task appears as a line in the NetShield Console window.

{button ,AL(`about on-access;about on-demand scan',0,`',`')} Related Topics

What is the on-access Scan task?

The on-access task is the server monitoring task. It monitors incoming files (files copied to the server) and outgoing files (files copied from the server). The administrator may specify what files are scanned and how NetShield responds to infected files.

Tip

- The on-access task protects the server. What about files not copied to or from the server? Schedule an on-demand task to perform automatic scans of local and network drives.

What are on-demand scan tasks?

On-demand tasks are drive scanning tasks which may be configured to scan the local drives, network drives or even specific folders or files. The administrator may specify what files are scanned, how often a scan takes place, and how Scan responds to infected files.

Tips

- On-demand tasks perform drive scans. What about files being copied to and from the server in between scans? The on-access task protects the server by monitoring files copied to and from the server.

About scheduled tasks

A scheduled task is an on-demand task configured to run at times specified by the administrator.

To create an on-demand task

1 Click  or select New Task from the Scan menu. A new scan task is created in the Console task window.

2 Type in a new name for the task and press ENTER. The task is created and the ScanConfig properties sheet appears. You are ready to configure this task.

Tip

To quickly create a new task, use the Scan Wizard. To start the Scan Wizard, click  or select Scan Wizard from the Scan menu and follow the instructions.

{button ,AL(`ODT',0,`',`')} Related Topics

To Configure an on-demand task

1 Highlight the task to configure.

2 Click  or select Properties from the Edit menu.
The ScanConfig properties sheet appears with the Action page displayed. You are ready to configure this task.

{button ,AL(`ODT',0,`',`')} Related Topics

Overview: Selecting files to scan

NetShield offers flexibility in choosing files to scan. By adding drives, folders, or specific files, you can configure a scan to be very focused on a small number of drives or folders that are very susceptible to viruses or you can configure a wide scan to search the entire network.

In addition to searching specific drives, Scan can check all files or only specified file types that are more susceptible to viruses. Setting Scan to check specified file types results in faster scanning.

Tip

- A good strategy for protecting your network is to focus highly susceptible areas (BBSs, Intranets, download directories, and areas with a lot of file activity) to frequent scans and perform complete network scans on a more infrequent basis.

{button ,AL(`Adding files to scan (on-demand)',0,`',`')} Related Topics

To add files to scan

1 Select the detection page from the ScanConfig properties sheet.
2 Click **Add**.
3 Select the files to scan.
To scan all network drives, select All Network Drives.
To scan all local drives, select All Local Drives.
To scan specific folders and files, Select Folders and Files.
4 If you selected Folders and Files, continue to Step 5. If you selected any other option, click **OK** and skip to Step 6.
5 Enter the path to the file or folder to scan or click **Browse** to choose a folder. Click **OK**. The new item appears in the Detection window.
6 Repeat Steps 1 through 5 until all scan items are entered.
7 Select the types of files to scan. To scan all file types, click the **All Files** radio button. To scan files with specific extensions, click the **Program Files** Only radio button.
8 To include the scanning of subfolders, check Include Subfolders.
9 To include scanning of compressed files, check the **Compressed Files** checkbox.
10 To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`ODT;FILODT',0,`',`')} Related Topics

To Edit a Scan item

1 Select the Detection page from the ScanConfig properties sheet.
2 Highlight an item and click **Edit**.
3 Select the files to scan.
To scan all network drives, select All Network Drives.
To scan all local drives, select All Local Drives.
To scan specific folders and files, Select Folders and Files.
4 If you selected Folders and Files, continue to Step 5. If you selected any other option, click **OK** and skip to Step 7.
5 Enter the path to the file or folder or click **Browse** to choose a folder.
6 Click **OK**. The edited item appears in the Detection window.
7 To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`FILODT',0,`',`')} Related Topics

To Delete a Scan item

1 Select the Detection page from the ScanConfig properties sheet.
2 Highlight the Scan item to delete and click **Remove**.
3 To add items, click **Add**.

{button ,AL(`FILODT',0,`',`')} Related Topics

To set how Scan responds to a virus

1 Select the Action page from the ScanConfig properties sheet.
2 Set how Scan responds to an infected file:
{button ,JI(`SHIELD.HLP',`Prompts_for_Action')} Scan prompts you for action
{button ,JI(`SHIELD.HLP',`Continues_Scanning')} Scan continues scanning
{button ,JI(`SHIELD.HLP',`Cleans_the_infected_file')} Scan cleans the infected file
{button ,JI(`SHIELD.HLP',`Deletes_the_infected_file')} Scan deletes the infected file

{button ,AL(`ODT',0,`',`')} Related Topics

Overview: Setting how Scan responds to a virus

Scan can be configured to respond to infected files by prompting you for action, by continuing to scan and taking no action, by cleaning them, or by deleting them.

Note

- You may choose only one of these options.

{button ,AL(`odto;Setting how Scan responds to a virus',0,`',`')} Related Topics

To instruct Scan to prompt you for Action

1. To instruct Scan to sound an alert when a virus is encountered, check the **Sound Alert** checkbox.
2. To instruct Scan to display a custom message, check the **Display Message** checkbox and insert a custom message.
3. To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

To instruct Scan to continue scanning without taking any action

1 Select Continue Scanning.

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

Note

- This is not a recommended option. If used, make sure to use alert notification. Otherwise, NetShield ignores any viruses encountered.

To instruct Scan to automatically clean infected files

1 Select Clean Infected Files.

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

To instruct Scan to automatically delete infected files

1 Select Delete Infected Files.

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

Overview: Scheduling a task

Scan offers a very flexible scheduling interface which allows customization of scans to fit your company's needs. Scans can be configured to occur one time only, once an hour, once a day, once a week, once a month, or transparently at system startup.

Tips

- Are your systems on 24-hours a day? If so, schedule an All Network Drives scan late at night.
- Do you have good employees who have bad shareware habits? Schedule a daily virus scan of their hard drives.
- Protect your server by running an All Local Drives scan at system startup.

{button ,AL(`odto;Scheduling a task',0,`',`')} Related Topics

To Schedule a task

1 Select the Schedule page from the ScanConfig properties sheet.
2 Check the **Enable Scheduler** checkbox.
3 Select the type of schedule to configure.

{button ,JI(`SHIELD.HLP',`One_time_task')} One time task
{button ,JI(`SHIELD.HLP',`Hourly_task')} Hourly task
{button ,JI(`SHIELD.HLP',`Daily_task')} Daily task
{button ,JI(`SHIELD.HLP',`Weekly_task')} Weekly task
{button ,JI(`SHIELD.HLP',`Monthly_tasks')} Monthly task
{button ,JI(`SHIELD.HLP',`Task_that_runs_at_Startup')} Task that runs at system startup

{button ,AL(`ODT',0,`',`')} Related Topics

To schedule a one time task

1. Click the **Once** radio button.
2. Enter the month, day, and time to start the task.
3. To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the console, click **Cancel**.

To schedule an hourly task

1 Click the **Hourly** radio button.

2 Set the task to start X minutes after the hour where X is a number between 0 and 59. For example, to instruct Scan to begin the task 30 minutes after every hour, type in '30'.

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

To schedule a daily task

1 Click the **Daily** radio button.

2 Click the **Which Days** button.

The Select Days dialog box appears.

4 Select which day(s) the task runs (ie. Sunday, Monday, etc.) and click **OK**.

5 Enter the time to start the task in the Start At field.

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

To schedule a weekly task

1. Click the **Weekly** radio button.
2. Enter the day and time to start the task.
3. To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the console, click **Cancel**.

To schedule a monthly task

1. Click the **Monthly** radio button.
2. Enter the day of the month and time to start the task.
3. To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the console, click **Cancel**.

To schedule a task that runs transparently at Startup

1 Click the **Startup** radio button.

2 To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the console, click **Cancel**.

Overview: Excluding files and folders from scanning

Scan may be configured to exclude specified folders or files from scanning.

Tip

- Configure Exclusions to exclude read-only directories, data files, restricted areas where risk of infection is low, and quarantine areas.

{button ,AL(`Adding a file or folders to exclude;odto',0,`',`')} Related Topics

To add a file or folder to exclude

1 Select the Exclusions page from the ScanConfig properties sheet.
2 To select files or folders to exclude from scanning, click **Add**.
The Exclude Item dialog box appears.
3 Enter the path to the file or folder or click **Browse** to select a folder.
4 To exclude subfolders from scanning, check the **Include Subfolders** checkbox.
5 To exclude the item from file scanning, make sure the **File Scanning** checkbox is checked.
6 To exclude the item from boot record scanning, check the **Boot Record Scanning** checkbox.
7 Click **OK**.
8 Repeat Steps 2 through 6 until all exclude items are entered.
9 To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`EXCODT',0,`',`')} Related Topics

To edit an exclude item

1. Select the Exclusions page from the ScanConfig properties sheet.
2. Highlight the exclude item and click **Edit**.
3. Enter a new path to a file or folder or click **Browse** to select a folder.
4. To exclude subfolders from scanning, check the **Include Subfolders** checkbox.
5. To exclude the item from file scanning, make sure the **File Scanning** checkbox is checked.
6. To exclude the item from boot record scanning, check the **Boot Record Scanning** checkbox.
7. Click **OK**.
8. To add an exclude item, click **Add**.
9. To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`EXCODT',0,`',`')} Related Topics

To delete an exclude item

1 Select the Exclusions page from the ScanConfig properties sheet.
2 Highlight the exclude item to delete and click **Remove**.
3 To add an exclude item, click **Add**.
4 To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`EXCODT',0,`',`')} Related Topics

Overview: Creating a virus activity log file

If enabled, NetShield NT keeps a virus activity log file. The log file keeps records of virus activity such as virus detection, virus cleaning, and infected file deletion. You may also choose to append information to the log such as the session settings, the session summary, the date and time, and the user name.

Tip

- To limit the size of the log file, select the limit log file size option and set the maximum size.

{button ,AL(`Creating a virus activity log file;odto',0,`',`')} Related Topics

To create a virus activity log file

1 Select the Reports page from the ScanConfig properties sheet.
2 Check the **Log to File** checkbox. The default log file location is C:\Win32app\NetShieldNT\ActivityLog.txt. Click **Browse** to choose a different location.
3 To limit the size of the log file, check the **Limit Size** checkbox and enter the maximum file size (in kilobytes).
4 Choose the type of activity to include in the log file. To include an activity, check its checkbox.
5 To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`ODT',0,`',`')} Related Topics

To Create the on-access task

The on-access task appears in the Console window and is preceded by a shield(). The on-access task cannot be created or deleted. To configure the on-access task, see Configuring the on-access task.

{button ,AL(`OAT',0,`',`')} Related Topics

To configure the on-access task

1 Highlight the on-access task.

2 Click  or select Properties from the Edit menu.
The ScanConfig properties sheet appears with the Action page displayed. You are ready to configure this task.

{button ,AL(`OAT',0,`',`')} Related Topics

Overview: Selecting files and file types to scan

When configuring the on-access task, be sure to check both Inbound and Outbound checkboxes.

Tip

- To improve scan performance, configure NetShield to only check specified file types which are likely to be infected (.EXE,.DLL,.COM).

{button ,AL(`odta;Selecting files and file types to scan',0,`',`')} Related Topics

To select files and file types to scan

1 Select the Detection page from the ScanConfig properties sheet.
2 Check the Inbound Files and the Outbound Files checkboxes.
3 Select the types of files to scan:
To scan all files, click the **All Files** radio button.
To scan files with specific extensions, click the **Program Files** Only radio button.
4 To include checking of compressed files, check the **Compressed Files** checkbox.
5 To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`OAT',0,`',`')} Related Topics

Program Files

Program files are file types which are most susceptible to viruses. By default, program files include files with the following extensions:

.EXE

.COM

.DLL

.SYS

.DO?

1 To add additional file types, click the **Program Files Only** radio button and click **Program Files**.

2 Click **Add**.

3 Enter a new extension to scan and click **OK**.

Overview: Setting how NetShield NT responds to a virus

NetShield NT may be configured to clean infected files, delete infected files, move infected files to a folder for quarantine, or deny access to infected files.

Note

- You may choose only one of these options.

{button ,AL(`odta;Setting how NetShield NT reponds to a virus',0,`',`')} Related Topics

To set how NetShield NT reponds to a virus

1 Select the Action page from the ScanConfig properties sheet.
2 Select how NetShield responds to an infected file.

{button ,JI(`SHIELD.HLP',`NetShield_cleans_the_infected_files')} Cleans the infected files
{button ,JI(`SHIELD.HLP',`NetShield_deletes_the_infected_files')} Deletes the infected files
{button ,JI(`SHIELD.HLP',`NetShield_moves_the_infected_files_to_a_folder')} Moves the infected files to a folder
{button ,JI(`SHIELD.HLP',`NetShield_denies_access_to_the_infected_files')} Denies access to the infected files

{button ,AL(`OAT',0,`',`')} Related Topics

To clean infected files

1 Select Clean Infected Files.

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

{button ,AL(`RESOAT',0,`',`')} Related Topics

To delete infected files

1 Select Delete Infected Files.

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

{button ,AL(`RESOAT',0,`',`')} Related Topics

To move infected files to a folder

1 Select Move Infected Files to a Folder
2 Enter a folder for the infected files or click **Browse** to choose a folder. Click **OK**.
3 To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

Tip

- To help keep track of virus origination, the path to the file is duplicated in the quarantine folder.

{button ,AL(`RESOAT',0,`',`')} Related Topics

To deny access to infected files

1 Select Deny Access to Infected Files.

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

{button ,AL(`RESOAT',0,`',`')} Related Topics

Overview: Excluding files from scanning

Scan may be configured to exclude specified folders or files from scanning.

Tip

- If you set NetShield to move infected files to a folder, exclude the folder from scanning.

{button ,AL(`Adding a file or folders to exclude;odta',0,`',`')} Related Topics

To add a file or folder to exclude from scanning

1. Select the Exclusions page from the ScanConfig properties sheet.
2. To select files or folders to exclude from scanning, click **Add**. The Exclude Item dialog box appears.
3. Enter the path to the file or folder or click **Browse** to select a folder.
4. To exclude subfolders from scanning, check the **Include Subfolders** checkbox.
5. Be sure the **Inbound Files** and **Outbound Files** checkboxes are checked.
6. Click **OK**.
7. Repeat Steps 2 through 6 until all exclude items are entered.
8. To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`EXCOAT;OAT',0,`',`')} Related Topics

To Edit an exclude item

1 Select the Exclusions page from the ScanConfig properties sheet.
2 Highlight the exclude item and click **Edit**.
3 Enter a new path to a file or folder or click **Browse** to select a folder.
4 To exclude subfolders from scanning, check the **Include Subfolders** checkbox.
5 Be sure the **Inbound Files** and **Outbound Files** checkboxes are checked.
6 Click **OK**.
7 To add an exclude item, click **Add**.
8 To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`EXCOAT',0,`',`')} Related Topics

To delete an exclude item

1 Select the Exclusions page from the ScanConfig properties sheet.
2 Highlight the exclude item to delete and click **Remove**.
3 To add an exclude item, click **Add**.
4 To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`EXCOAT',0,`',`')} Related Topics

Overview: Creating a virus activity log file

If enabled, NetShield NT keeps a virus activity log file. The log file keeps records of virus activity such as virus detection, virus cleaning, infected file deletion, and infected file move. You may also choose to append information to the log, such as: the session settings, session summary, date and time, and the user name.

Tip

- To limit the size of the log file, select the limit log file size option and select the maximum size.

{button ,AL(`Creating a virus activity log file (oa);odta',0,`',`')} Related Topics

To create a virus activity log file

1 Select the Reports page from the ScanConfig properties sheet.
2 Check the **Log to File** checkbox. The default log file location is C:\Win32app\NetShieldNT\ActivityLog.txt. Click **Browse** to choose a different location.
3 To limit the size of the log file, check the **Limit Size** checkbox and enter the maximum file size (in kilobytes).
4 Choose the type of activity to include in the log file. To include an activity, check its checkbox.
5 To further configure this task, select another properties page. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`OAT',0,`',`')} Related Topics

To set NetShield to load at startup

This option automates virus protection. When enabled, the McAfee Task Manager Service automatically starts at system startup.

1 Select the Detection page from the ScanConfig properties sheet.

2 Check the **Load NetShield at startup** checkbox.

To allow disabling of the on-access task

Normally, the on-access task cannot be disabled from the Console. To allow disabling of the task:

1 Select the Detection page from the ScanConfig properties sheet.

2 Check the **NetShield can be disabled** checkbox.

To view the status of a scan

Choose a task to view and double-click the task.

The Statistics screen appears. From this screen you can watch the status of a scan including information on the number of files scanned and the number of infected files encountered.

Connecting to another computer

The NetShield NT Console can administer any Server with the NetShield NT server component installed. To connect to a computer, complete the following procedure.

1 Click  or select Select Computer from the Tools menu.

2 Enter the name of the computer to administer or click **Browse** to locate the computer.

3 Click **Connect**.

If the service is not active on the computer, you are prompted to start it. Click **Start**.

4 You are ready to configure the computer.

5 To confirm the connection, check the Console title bar. The name of the computer being administered appears in the title bar of the Console.

6 To disconnect from the computer, click  or connect to another computer.

{button ,AL(`COMPCONN',0,`',`')} Related Topics

Copying tasks to another computer

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

1 Highlight the task you want to copy and click the **Copy** button or select Copy from the Edit menu.

2 Connect to the computer where you want to copy the task.

3 Click  or select Paste from the Edit menu.
The task is copied and appears as New Scan Task in the Console window.

4 Enter a name for the task and press ENTER.
The ScanConfig properties sheet appears.

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

Note

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

{button ,AL(`COMPCONN',0,`',`')} Related Topics

To start a task on another computer

1 Connect to another computer.

2 Highlight a task and click  or select Start from the Scan menu.
"Running" appears under "Status" in the Console window.

3 To watch the progress of the Scan, double-click the task or select Statistics from the Scan menu. The Statistics screen appears.

{button ,AL(`COMPCONN',0,`',`')} Related Topics

Overview: Using AutoUpdate to keep NetShield NT updated

AutoUpdate is a powerful feature which can ensure you always have the latest version of the anti-virus data files on your systems.

For example, a script could download the latest Updates from the McAfee ftp site or the McAfee Bulletin Board System. After the Update is downloaded, AutoUpdate can store the Update for distribution. Then, you can configure other NT systems to download updates from the distribution site.

{button ,AL(`auto',0,`',`')} Related Topics

Obtaining Updates from McAfee

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

{button ,JI(`SHIELD.HLP',`McAfee_bulletin_board_system_BBS')} McAfee bulletin board system (BBS)

{button ,JI(`SHIELD.HLP',`McAfee_Forum_on_CompuServe')} McAfee Forum on CompuServe

{button ,JI(`SHIELD.HLP',`Internet_Access')} Internet Access

{button ,AL(`auto',0,`',`')} Related Topics

To obtain Updates using scripts

1 Select AutoUpdate from the Tools menu.
The AutoUpdate properties sheet appears with the Update Location page displayed.
2 Click the **Obtain Update Module using shell script** radio button and enter the location of the update module.
3 To perform the update now, click **Update Now**.
4 To schedule AutoUpdate, click the Schedule tab.

{button ,AL(`auto;Using scripts for updates',0,`',`')} Related Topics

To obtain Updates from distribution points

1 Select AutoUpdate from the Tools menu.
The AutoUpdate properties sheet appears with the Update Location page displayed.
2 Click the **Copy update module from distribution** radio button and enter the location of the shell script.
3 To perform the update now, click **Update Now**.
4 To schedule this script, click the Schedule tab.

{button ,AL(`auto',0,`',`')} Related Topics

To Schedule an AutoUpdate

1 Select AutoUpdate from the Tools menu.
2 Configure the AutoUpdate options on the Update Location page.
3 Select the Schedule page from the AutoUpdate properties sheet.
4 Check the **Enable Scheduler** checkbox.
5 Select the type of schedule to configure.

{button ,JI(`SHIELD.HLP',`To_schedule_a_one_time_update')} One time update
{button ,JI(`SHIELD.HLP',`To_schedule_a_hourly_update')} Hourly update
{button ,JI(`SHIELD.HLP',`To_schedule_a_daily_update')} Daily update
{button ,JI(`SHIELD.HLP',`To_schedule_a_weekly_update')} Weekly update
{button ,JI(`SHIELD.HLP',`To_schedule_a_monthly_update')} Monthly update
{button ,JI(`SHIELD.HLP',`To_schedule_an_update_that_runs_transparently_at_Startup')} Update that runs at system startup

{button ,AL(`auto',0,`',`')} Related Topics

To schedule a one time update

1 Click the **Once** radio button.
2 Enter the month, day, and time to start the update.
3 For further configuration, click the Update Location tab. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`UPSSCH',0,`',`')} Related Topics

To schedule a hourly update

1 Click the **Hourly** radio button.
2 Set the update to start X minutes after the hour where X is a number between 0 and 59. For example, to instruct Scan to begin the update 30 minutes after every hour, type ‘30’.
3 For further configuration, click the Update Location tab. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`UPSSCH',0,`',`')} Related Topics

To schedule a daily update

1 Click the **Daily** radio button.
2 Click the Which Days button.

The Select Days dialog box appears.

4 Select which day(s) the update runs (ie: Sunday, Monday, etc.) and click **OK**.
5 Enter the time to start the task in the Start At field.
6 For further configuration, click the Update Location tab. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`UPSSCH',0,`',`')} Related Topics

To schedule a weekly update

1 Click the **Weekly** radio button.
2 Enter the day and time to start the update.
3 For further configuration, click the Update Location tab. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`UPSSCH',0,`',`')} Related Topics

To schedule a monthly update

1 Click the **Monthly** radio button.
2 Enter the day of the month and time to start the update.
3 For further configuration, click the Update Location tab. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`UPSSCH',0,`',`')} Related Topics

To schedule an update that runs transparently at Startup

1 Click the **Startup** radio button.
2 For further configuration, click the Update Location tab. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`UPSSCH',0,`',`')} Related Topics

To Store Updates for distribution

After retrieving an update, AutoUpdate can store the update module in a location accessible by all servers running NetShield NT. To configure AutoUpdate to store update modules for distribution, complete the following procedure:

1 Check the **Store Update** checkbox.

2 Enter the path to the distribution location or click **Browse** to choose a folder.

3 For further configuration, select other options. To save the changes and return to the Console, click **OK**. To cancel any changes and return to the Console, click **Cancel**.

{button ,AL(`auto',0,`',`')} Related Topics

Overview: Alert Manager

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

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

Note

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

{button ,AL(`alert',0,`',`')} Related Topics

Viewing the Summary page

The Summary page lists all alert notification items.
From this page, view the properties or remove an alert notification item.

{button ,AL(`alert',0,`',`')} Related Topics

To open the Alert Manager Properties window

1 Select Alerts from the Tools menu.
The Alert List properties sheet appears.

2 Check the **Send events to Alert Manager** checkbox and click **Configure**.
The Alert Manager properties sheet appears with the Summary page showing.

{button ,AL(`alert',0,`',`')} Related Topics

Forwarding alerts to a computer

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

1 Open the Alert Manager properties sheet.
2 Select the Forward page.
The Forward page appears with a list of all systems configured to receive forwarded messages.
3 To add a computer to receive forwards, click **Add**.
4 Specify a computer or click **Browse** to locate the computer.
5 To test the forward, click **Test**.
The computer receives a test message.
6 To set the priority level of the messages this e-mail address receives, click **Priority Alerts**.
To set the address to receive low, medium, and high priority alerts, select Low.
To set the address to receive medium and high priority alerts, select Medium.
To set the address to receive high priority alerts only, select High.
7 Click **OK**.
8 To add another computer to receive forwarded alerts, click **Add**.
9 To configure other notification options, select another properties page. To save the changes and exit, click **OK**.
To cancel any changes, click **Cancel**.

Note

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

Tip

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

{button ,AL(`alop',0,`',`')} Related Topics

To send network message alerts

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

1 Open the Alert Manager properties sheet.

2 Select the Network Message page.
The Network Message page appears with a list of all systems configured to receive network messages.

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

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

5 To test the connection, click **Test**.
The message recipient receives a test message.

6 To set the priority level of the messages this computer receives, click **Priority Alerts**.
To set the system to receive low, medium, and high priority alerts, select Low.
To set the system to receive medium and high priority alerts, select Medium.
To set the system to receive high priority alerts only, select High.

7 Click **OK**.

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

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

{button ,AL(`alop',0,`',`')} Related Topics

To send alerts to an e-mail address

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

1 Open the Alert Manager properties sheet.

2 Select the E-Mail page.
The E-Mail page appears with a list of e-mail addresses configured to receive alert notifications.

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

4 Enter an e-mail address, fill out the Subject line, and fill out the From line.

5 To configure SMTP settings, click **Configure SMTP** and enter the name of the Server and Login.

6 To test the connection, click **Test**.
The message recipient receives a test message.

7 To set the priority level of the messages this e-mail address receives, click **Priority Alerts**.
To set the address to receive low, medium, and high priority alerts, select Low.
To set the address to receive medium and high priority alerts, select Medium.
To set the address to receive high priority alerts only, select High.

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

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

{button ,AL(`alop',0,`',`')} Related Topics

To send alerts to a pager

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

1 Open the Alert Manager properties sheet.

2 Select the Pager page.
The Pager page appears with a list of all pagers configured to receive alert notifications.

3 To add a pager , click **Add**.

4 Select the type of pager:

{button ,JI(`SHIELD.HLP',`Alphanumeric_pager')} Alphanumeric pager

{button ,JI(`SHIELD.HLP',`Numeric_pager')} Numeric pager

{button ,AL(`alop',0,`',`')} Related Topics

Alphanumeric pager

To configure an alphanumeric pager:

1 Enter the pager phone number, enter an ID or a PIN number (if applicable), and enter a password (if applicable).

2 To use the standard alert message, click the **Use standard alert message** radio button.

3 To use a custom message, click the **Use custom alert message** radio button and enter a message in the following field.

4 Click **Modem** to configure the modem settings.

5 To test the pager, click **Test**.

6 To set the priority level of alert notifications this pager receives, click **Priority Alerts**.
To set the address to receive low, medium, and high priority alerts, select Low.
To set the address to receive medium and high priority alerts, select Medium.
To set the address to receive high priority alerts only, select High.

7 Click **OK**.

8 To add another pager to receive notifications, click **Add**.

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

Numeric pager

To configure a numeric pager:

1 Enter the pager phone number.

2 Enter a numeric message.

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

4 Click **Modem** to configure the modem settings.

5 To test the pager, click **Test**.

6 To set the priority level of alert notifications this pager receives, click **Priority Alerts**.
To set the address to receive low, medium, and high priority alerts, select Low.
To set the address to receive medium and high priority alerts, select Medium.
To set the address to receive high priority alerts only, select High.

7 Click **OK**.

8 To add another pager to receive notifications, click **Add**.

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

To send alerts to a printer

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

1 Open the Alert Manager properties sheet.

2 Select the Printer page.
The Printer page appears with a list of all systems currently configured to receive alert notifications.

3 To add a printer, click **Add**.

4 Click **Browse** to locate the printer.

5 To test the connection, click **Test**.
The printer prints a test message.

6 To set the priority level of the messages this printer receives, click **Priority Alerts**.
To set the system to receive low, medium, and high priority alerts, select Low.
To set the system to receive medium and high priority alerts, select Medium.
To set the system to receive high priority alerts only, select High.

7 Click **OK**.

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

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

Note

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

{button ,AL(`alop',0,`',`')} Related Topics

To use SNMP

The Alerts Manager supports SNMP. To enable SNMP, complete the following procedure.

1 Open the Alert Manager properties sheet.

2 Select the SNMP page.
The SNMP page appears.

3 Check the **Enable SNMP** checkbox.

4 To configure SNMP services, click **Configure**.
The Microsoft NT Network Settings properties sheet appears.

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

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

{button ,AL(`alop',0,`',`')} Related Topics

To customize alerts

1 Select Alerts from the Tools menu.
2 Click the Messages tab. The Messages page appears.
3 To enable an alert, highlight an alert item and check its checkbox.
4 To change the priority of an alert, highlight the alert item and click **Edit**. The Alert Properties dialog box appears. Set the new priority level in the Priority field and click **OK**.
5 To change an alert message, highlight an alert item and click **Edit**. The Alert Properties dialog box appears. Enter a new message in the Message field and click **OK**.

{button ,AL(`alert;message variables (Reference)',0,`',`')} Related Topics

To log alerts in the application log

1 Select Alerts from the Tools menu.
2 Check the **Log Event** checkbox.
3 To log alert events in the local computer's event log, click the **Use local computer** radio button.
4 To log alert events in another computer's event log, click the **Use another computer** radio button. Click **Browse** to locate the computer.
5 Click **OK**. Alert events arestored in the Application Log.

{button ,AL(`alert',0,`',`')} Related Topics

To Execute a program on alert

1 Select Alerts from the Tools menu.
2 Check the **Execute program on event** checkbox.
3 Enter the name and path of the program to execute or click **Browse** to locate the program.
4 To execute the program every time an alert event occurs, click the **Every Time** radio button. To execute the program on the first alert event only, click the **First Time** radio button.
5 To save the changes and return to the console, click **OK**. To cancel any changes, click **Cancel**.
6 For more information on executing programs on alert, see Launching Programs on Alerts.

{button ,AL(`alert;Launching programs upon alerts',0,``',`')} Related Topics

Technical Support

For help using this product, please contact McAfee technical support. McAfee technical support is available:

On-line 24 hours a day, through our bulletin board system, CompuServe, or Internet (see "On-line access to updates and technical support" below).

By fax at (408) 970-9727.

By telephone at (408) 988-3832, Monday through Friday, 6:00 AM to 5:00 PM Pacific Standard Time.

For fast and accurate help, please have the following information ready:

- Program name and version number.
- Type and brand of computer.
- Version of Windows NT.
- List of other Services loaded on your server.
- A description of the exact problem. Please be as specific as possible.

If you are overseas, 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. Please refer to the AGENTS.TXT file for a complete list of McAfee agents.

Overview: On-line access to updates

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

{button ,JI(`SHIELD.HLP',`McAfee_bulletin_board_system_BBS')} McAfee bulletin board system (BBS)

{button ,JI(`SHIELD.HLP',`McAfee_Forum_on_CompuServe')} McAfee Forum on CompuServe

{button ,JI(`SHIELD.HLP',`Internet_Access')} Internet Access

McAfee bulletin board system (BBS)

Our multi-line 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. 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. A free introductory membership is available. For more information, please read the enclosed COMPUSER.TXT file.

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.

McAfee's anti-virus software is also available on 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).

Preventing viruses

Although McAfee NetShield is designed to offer the highest degree of virus protection, detection and eradication available, no anti-virus program can prevent all computer viruses. Even with frequent updates, new viruses currently appear at a rate of three to four a day, and this number may grow even higher in the future.

Keeping your anti-virus software current is one way to prevent the overwhelming majority of computer viruses from infecting your system. However, following the steps listed below can greatly reduce the chance of becoming infected.

Never boot your PC with a floppy diskette in Drive A:

Although boot viruses only account for approximately 10% of the total number of computer viruses, they account for over 90% of reported virus infections. **All** formatted diskettes, even data diskettes, contain a boot sector the computer attempts to execute when started. Even if this attempt is unsuccessful, a virus in the boot sector is read into memory and executed, at which point it can infect the hard disk.

Use software only from reputable sources

When purchasing commercial software, be sure the software is in its original packaging and was not previously used and returned.

When using BBSs, check with the Systems Operator about their scanning procedures. Many System Operators scan for viruses before making files available for downloading.

Most commercial electronic services such as CompuServe and America Online scan files for viruses before making them available for downloading.

Scan all incoming disks and files for viruses

Scan all diskettes and files you receive for viruses before using them. This includes: purchased programs, downloaded programs, demonstration diskettes, diskettes from friends and coworkers, and your diskettes after they have been used in another computer.

{button ,AL(`Making regular backups',0,`',`')} Related Topics

Making regular backups

Some viruses may leave certain disks or files unusable even after they are cleaned and some infections involve files which are corrupted beyond repair.

To increase your chance of recovery, periodically back up all files located on hard disks onto clean backup media. Scan the backup program disk first to ensure the backup program itself is not infected. Do not run the backup program if it is infected.

Although some of the backed-up files may be infected, it is better to have current copies than none at all. However, do not overwrite previous backup disks or tapes, which may be uninfected.

{button ,AL(`Preventing viruses',0,`',`')} Related Topics

Using scripts for updates

Reaching a service

AutoUpdate can be configured to use a script to retrieve the latest NetShield updates. These updates may contain virus data files, program files, or both.

The script file must be written to accept a command line argument from the AutoUpdate module. Configure the script to do the following:

- Log into the service (BBS, FTP, Web page, or proprietary location).
- Navigate to the location of the update files.
- Setup file transfer protocols.
- Download the file specified on the command line.

Downloading the update

Download VERSION.DAT. This file contains the name of the latest Update Module and determines if your version of NetShield is current enough to use it. If your version qualifies, AutoUpdate uses the script to download the update module.

Sample Script - FTPGET.CMD and VERSION.DAT

Sample ftp script

```
rem Create FTP command file FTPCMD.FTP
echo open>FTPCMD.FTP
echo ftp.mcafee.com>>FTPCMD.FTP
echo ftp>>FTPCMD.FTP
echo %USERNAME%@%USERDOMAIN%>>FTPCMD.FTP
echo bin>>FTPCMD.FTP
echo get /pub/updates/%1>>FTPCMD.FTP
echo close>>FTPCMD.FTP
echo quit>>FTPCMD.FTP

rem Now launch ftp.exe with the command file FTPCMD.FTP
ftp -s:FTPCMD.FTP >> FTPGET.LOG
rem Now delete FTPCMD.FTP
del FTPCMD.FTP > nul
rem We're done
```

Sample VERSION.DAT

```
[NetShield]
uVersion=251
uVersionReq=250
szUpdateModule=datupd.exe
```

The above sample creates and opens the temporary file FTPCMD.FTP, loads the command lines necessary to access the McAfee ftp site, downloads VERSION.DAT, and checks that you currently have version 2.50 (250). If you have version 2.50, VERSION.DAT feeds the name of the update (DATUPD.EXE) to AutoUpdate. AutoUpdate then downloads the Update and updates the version to 2.51 (251).

Note

This is a sample script only. Do not use this sample without modification.

Remote administration

Viewing remote log files

The Activity Log file cannot be remotely viewed unless the log file location is defined using the UNC standard.

Remotely starting a scan task

When starting a remote task, Scan's GUI interface is not visible.

Launching programs upon alerts

In the event that Alert Manager does not meet your needs, you can configure it to launch any program or batch file on alert.

Note

- Any program launched from the Alert Manager runs in the background.

Tip

- If your company is using cc:Mail or a special mail package that is not recognized by McAfee, write a batch file to send notifications to your mail package.

Using Windows 95 to administer NetShield

The Console component is designed to run on Windows 95, Windows NT Server, or Windows NT Workstation. From Windows 95, you can administer Windows NT Servers running NetShield NT and/or Workstations running VirusScan NT.

To administer NetShield from Windows 95:

1 Install the NetShield Console. See the NetShield NT User's Manual.

2 Select the Console icon in the McAfee NetShield NT Group.

3 When prompted, enter the system to administer or click **Browse**.

Scan found a virus

If NetShield does locate a virus, DO NOT panic! NetShield will react automatically or prompt you to determine the next step, depending on how you set the Actions property page. In most cases, NetShield will quickly and easily disinfect your system to the next step.

{button ,JI(`SHIELD.HLP',`Virus_found_Clean_infected_file')} Clean infected file

{button ,JI(`SHIELD.HLP',`Virus_found_Delete_infected_file')} Delete infected file

{button ,JI(`SHIELD.HLP',`Virus_found_Move_infected_file_to_a_folder')} Move infected file to a folder

{button ,JI(`SHIELD.HLP',`Virus_found_Prompt_for_action')} Prompt for action

{button ,JI(`SHIELD.HLP',`Virus_found_Continue_scanning')} Continue scanning

Virus found: Clean infected file

Automatically attempts to clean the contaminated file. In most cases, NetShield will fully restore the file to its virus-free state. Yet in some cases, such as overt file corruption, NetShield cannot perform this function. In this case, NetShield denies access to the file and you will be informed the cleaning was unsuccessful.

Tips

- To customize notification methods, see Overview: Alerts Manager.
- To learn more about your virus, see Viewing the virus list.

Virus found: Delete infected file

Automatically deletes the contaminated file and records this action in the log file. After deletion, you must obtain the original file (possibly from backup). We recommend scanning your backup copy to ensure your file will not be re-corrupted.

Tip

- To learn more about your virus, see Viewing the virus list.

Virus found: Move infected file to a folder

Automatically moves the infected file to a folder and records this action in the log file. The path to the file is duplicated in the quarantine folder.

Tips

- Exclude the quarantine folder from scanning on the Exclusions properties page.
- To prevent re-infection, deny access to this folder.
- To learn more about your virus, see Viewing the virus list.

Virus found: Prompt for action

If a virus is found and the Action property page is set to Prompt for Action, you will be given several options on how to react.

- Choose Continue to scan the remainder of your selection.
- Choose Stop to end the scan session.
- Choose Clean to disinfect the file.
- Choose Delete to erase the file.

Tips

- To learn more about your virus, see Viewing the virus list.
- To learn more about your virus, see Viewing the virus list.

Virus found: Continue scanning

If you selected this option, it will continue scanning until it found all viruses and searched all specified file locations.

Note

- This is not a recommended option. If used, make sure to use alert notification. Otherwise, NetShield ignores any viruses encountered.

Tip

- To learn more about your virus, see Viewing the virus list.

Boot sector is infected

Boot sector viruses can only be passed through booting from a floppy disk. If a system has a boot sector virus infection, it is unlikely the system will reboot.

To clean a boot sector virus, reboot the system using the McAfee Emergency Recovery diskette.

Tip

- To learn more about your virus, see Viewing the virus list.

Unable to connect to another computer

NetShield NT utilizes Windows NT's built-in security. If you are ability to administer remote systems with native NT tools, you can remotely administer NetShield.

If you are having problems in connecting, check the following:

- Confirm NetShield is installed on the remote system.
- Use Microsoft's Registry Editing tool, REGEDT32.EXE, to view/edit the remote system's registry. If you can view the registry, NetShield should be able to connect to the remote system.
- Check network protocols and confirm they are consistent on both the local and the remote system.

We 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 may provide useful information about viruses:

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

NetShield for Windows NT User's Manual

Click here  to open the NetShield for Windows NT User's Manual.

Note

- You must have Adobe Acrobat installed to view the manual.

Commandline options

Usage

SCAN32 [<switches>] [<scanitem>]
SCAN32 <config.VSC> [<override_switches>] [<override_scanitem>]
SCAN32 [/SERVER <servername>] /TASK <**taskid> [<override_switches>]** [<override_scanitem>]

Command Line Switches

/[NO]SPLASH Default: /SPLASH
Displays initial splash screen.

/[NO]AUTOSCAN Default: <depends on UI type>
Scan32 automatically initiates scanning when started.

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

/[NO]ALWAYSEXIT Default: <depends on UI type>
Scan32 automatically exits when scan is complete. Scan32 exits even if viruses are detected (see /AUTOEXIT).

/[NO]SUB Default: /SUB
Use this switch to scan all subfolders.

/[NO]ALL Default: /NOALL
Scans all files, regardless of their file extension.

/[NO]COMP Default: /COMP
Scans compressed files and ZIP files.

/UICONFIG | /UIEXONLY | /UINONE Default: /UICONFIG
Specifies the type of graphical user interface displayed:

- UICONFIG - A fully-configurable interface which allows the user to specify which items to scan.
- UIEXONLY - An "execution-only" interface which takes all options from the command line, registry or VSC file. This value implies /AUTOSCAN and /AUTOEXIT.
- UINONE - No visible user interface. All options must be taken from the command line, registry or VSC file. Activity logging should be used to obtain the scan results. This value implies /AUTOSCAN and /ALWAYSEXIT.

/CONTINUE | /PROMPT | /CLEAN | /DELETE | /MOVE <FOLDER> Default: /CONTINUE
Specifies what action to take when a virus is detected:

- CONTINUE - Logs information about the infection and continue scanning.
- PROMPT - Pauses the scan to ask the user which action to take (see /MSG).
- CLEAN - Attempts to clean the infected item and continue with the scan.
- DELETE - Attempts to delete the infected item and continue with the scan.
- MOVE - Attempts to move the infected files and continue scanning.

/[NO]MSG <message> Default: /NOMSG
Displays a custom message when the /PROMPT option is specified and a virus is detected.

/[NO]BEEP Default: /BEEP
Plays an audible tone on completion of a scan if infected items were found.

/RPTSIZE <n> Default: /RPTSIZE 100
Specifies the maximum size of the activity log file (in kilobytes). When the file exceeds this size, it is truncated to zero bytes.

/[NO]MEM Default: /MEM

Performs a memory scan.

/[NO]BOOT Default: /BOOT

Performs a boot record scan. The Master Boot Record (MBR) is scanned and the Boot Sector of each drive where a scan item resides is scanned.

/EXT extensions Default: /EXT "EXE COM BIN SYS DO? OVL DLL APP CMD"

List the file extension types to scan, unless the /ALL option is specified. To modify this list, the entire list must be entered with each entry separated by a space, for example: /EXT "EXE COM SYS ZIP".

/DEFEXT extensions Default: /DEFEXT "EXE COM BIN SYS DO? OVL DLL APP CMD PRG"

A list of program extensions to default to when user selects "New Scan" from the configurable (see /CONFIG) user interface. The entire list must be quoted and each entry separated by a space, for example: /DEFEXT "EXE COM SYS ZIP".

/PRIORITY <n> Default: /PRIORITY 3

Set the priority of the scan process using a value between 1 and 5.

/TASK <taskid> Default: (none)

Specifies:

(a) configuration data should be read from the registry.

- The taskid is a registry key found under: HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\VirusScan\Tasks.
- This parameter may be used with or without the /SERVER option. If /SERVER is omitted, the local registry is used.

(b) when used with the /CANCEL option, the task is terminated.

/SERVER <servername> Default: (none)

Specifies configuration data should be read from the registry on the specified server. The /TASK option must be used with this parameter.

/CANCEL Default: (none)

Specifies a running task should be canceled. The /TASK parameter must be used with this option to specify which task is to be canceled.

/[NO]LOG [<logfile>] Default: /LOG "VirusScan Activity Log.txt"

Enables activity logging and optionally, changes the name of the log file.

/LOGALL Default: /LOGALL

Specifies all scan activity is logged and it is equivalent to specifying /LOGDETECT /LOGCLEAN /LOGDELETE /LOGMOVE /LOGSETTINGS /LOGSUMMARY /LOGDATETIME /LOGUSER

/[NO]LOGDETECT Default: /LOGDETECT

Logs the detection of infected items.

/[NO]LOGCLEAN Default: /LOGCLEAN

Logs the results of attempts to clean infected items.

/[NO]LOGDELETE Default: /LOGDELETE

Logs the results of attempts to delete infected items.

/[NO]LOGMOVE Default: /LOGMOVE

Logs the results of attempts to move infected items.

/[NO]LOGSETTINGS Default: /LOGSETTINGS

Logs the list of configuration settings used for each scan.

/[NO]LOGSUMMARY Default: /LOGSUMMARY

Logs a summary of the completed scan.

/[NO]LOGDATETIME Default: /LOGDATETIME
Timestamps each entry in the log file.

/[NO]LOGUSER Default: /LOGUSER
Stamps each entry in the log file with the name of the user who executed the scan.

Not Supported

Exclusions
Multiple Scan Items

Overview: Scan

Scan is a standalone virus scanner which is useful for running simple virus scans.
To start Scan, double-click the Scan icon in the NetShield program group.

{button ,AL(`SCAN',0,`',`')} Related Topics

To select files to scan

1 Select the Where and What page from the Scan properties sheet.
2 Enter the path to the file or folder to scan or click **Browse** to choose a folder. Click **OK**. The location appears in the Scan In window.
3 To include the scanning of subfolders, check Include Subfolders.
4 Select the types of files to scan. To scan all file types, click the **All Files** radio button. To scan files with specific extensions, click the **Program Files** Only radio button.
5 To include scanning of compressed files, check the **Compressed Files** checkbox.
6 To further configure this task, select another properties page. To run this scan now, click **Scan Now**. To save these settings to run later, select Save Settings from the File menu.

{button ,AL(`SCAN',0,`',`')} Related Topics

To set how Scan responds to infected files

1 Select the Actions page from the Scan properties sheet.

2 Set how Scan responds to an infected file:

{button ,JI(`SHIELD.HLP',`Scan_prompts_you_for_Action')} Prompts you for action

{button ,JI(`SHIELD.HLP',`Scan_continues_scanning_without_taking_any_action')} Continues scanning without taking any action

{button ,JI(`SHIELD.HLP',`Scan_moves_infected_files_to_a_folder')} Automatically moves infected files to a folder

{button ,JI(`SHIELD.HLP',`Scan_automatically_cleans_infected_files')} Automatically cleans infected files

{button ,JI(`SHIELD.HLP',`Scan_automatically_deletes_infected_files')} Automatically deletes infected files

Note

- You may only choose one of these options.

{button ,AL(`SCAN',0,`',`')} Related Topics

To instruct Scan to prompt you for Action

1. Select Prompt for Action.
2. Enable the **Sound Alert** and **Display Message** options on the Reports page.
3. To instruct Scan to display a custom message, check the **Display Message** checkbox and insert a custom message.
4. To further configure this task, select another properties page. To run this scan now, click **Scan Now**. To save these settings to run later, select Save Settings from the File menu.

To instruct Scan to continue scanning without taking any action

1 Select Continue Scanning.

2 To further configure this task, select another properties page. To run this scan now, click **Scan Now**. To save these settings to run later, select Save Settings from the File menu.

Note

- This is not a recommended option. If used, make sure to use alert notification. Otherwise, NetShield ignores any viruses encountered.

To instruct Scan to automatically clean infected files

1 Select Clean Infected Files.

2 To further configure this task, select another properties page. To run this scan now, click **Scan Now**. To save these settings to run later, select Save Settings from the File menu.

To instruct Scan to automatically delete infected files

1 Select Delete Infected Files.

2 To further configure this task, select another properties page. To run this scan now, click **Scan Now**. To save these settings to run later, select Save Settings from the File menu.

To instruct Scan to move infected files to a folder

1 Select Move Infected Files to a Folder
2 Enter a folder for the infected files or click **Browse** to choose a folder. Click **OK**.
3 To further configure this task, select another properties page. To run this scan now, click **Scan Now**. To save these settings to run later, select Save Settings from the File menu.

Tip

- To help keep track of virus origination, the path to the file is duplicated in the quarantine folder.

To select how Scan reports virus activity

1. Select the Reports page from the Scan properties sheet.
2. To send a display message on virus detection, check the **Display Message** checkbox and enter a message.
3. To sound an alert on virus detection, check the **Sound Alert** checkbox.
4. To log virus activity in a log file, check the **Log to File** checkbox. The default log file location is C:\Win32app\NetShieldNT\ActivityLog.txt. Click **Browse** to choose a different location.
5. To limit the size of the log file, check the **Limit Size** checkbox and enter the maximum file size (in kilobytes).
6. To further configure this task, select another properties page. To run this scan now, click **Scan Now**. To save these settings to run later, select Save Settings from the File menu.

Note

- The **Display Message** option is only available if Prompt for Action is selected on the Actions page.

{button ,AL(`SCAN',0,`',`')} Related Topics

VSC file format

VSC files are used by SCAN32 to import and export tasks. The VSC file is a text file with a format similar to the Windows INI file. Each variable has a name followed by '=' sign and a value and are arranged in five groups.

[ScanOptions] - defines scanner options

Name: szProgramExtensions
Type: String
Defines extensions to be used as program extensions during scan
Default value: EXE COM DLL SYS DO?

Name: szDefaultProgramExtensions -
Type: String
Defines extensions to be used as default program extensions during scan configuration
Default value: EXE COM DLL SYS DO?

Name: bIncludeSubFolders
Type: Boolean (1/0)
Instructs scanner to search for viruses inside subfolders
Default value: 1

Name: bScanAllFiles
Type: Boolean (1/0)
Instructs program to scan inside all files
Default value: 0

Name: bScanCompressed
Type: Boolean (1/0)
Instructs program to scan inside compressed files (PkLite, LZEXE, ZIP)
Default value: 1

Name: uScanAction
Type: Integer (1-5)
Defines what action will be taken upon virus detection:
1 -
2 -
3 -
4 -
5 -
Default value: 1

Name: bAutoStart
Type: Boolean (1/0)
Defines if scan will be started immediately upon launch
Default value: 0

Name: bAutoExit
Type: Boolean (1/0)
Defines if scanner will be unloaded when scan is finished
Default value: 0

Name: nPriority=0
Type: Integer (0-5)
Defines the priority at which scan is to be executed
Default value: 3

Name: szScanItem=C:\
Type: String
Defines item to be scanned
Default value: C:\

[AlertOptions]

Name: bDisplayMessage
Type: Boolean (1/0)
Defines if custom message should be displayed upon virus detection.
Default value: 1

Name: szCustomMessage
Type: String
Defines custom message to be displayed upon virus detection.
Default value: Your custom message here!

Name: bSoundAlert
Type: Boolean (1/0)
Defines if audible alert should be made upon virus detection.
Default value: 1

[ActivityLogOptions]

Name: bLogToFile
Type: Boolean (1/0)
Defines if scan results should be logged into log file
Default value: 1

Name: bLimitSize
Type: Boolean (1/0)
Defines if size of the log file should be limited
Default value: 1

Name: uMaxKilobytes
Type: Integer
Defines maximum size of the log file
Default value: 100

Name: szLogFileName
Type: String
Defines log file name
Default value: VirusScan Activity Log.txt

Name: bLogDetection
Type: Boolean (1/0)
Defines if scan results should be logged
Default value: 1

Name: bLogClean
Type: Boolean (1/0)
Defines if clean results should be logged
Default value: 1

Name: bLogDelete
Type: Boolean (1/0)
Defines if infected file delete operations should be logged

Default value: 1

Name: bLogMove
Type: Boolean (1/0)
Defines if infected file move operations should be logged
Default value: 1

Name: bLogSettings
Type: Boolean (1/0)
Defines if session settings should be logged
Default value: 1

Name: bLogSummary
Type: Boolean (1/0)
Defines if session summary should be logged
Default value: 1

Name: bLogDateTime
Type: Boolean (1/0)
Defines if time and date of an event should be logged
Default value: 1

Name: bLogUserName
Type: Boolean (1/0)
Defines if user name should be logged
Default value: 1

[Scheduler]

Name: bSchedEnabled
Type: Boolean (1/0)
Enables scheduling for the task
Default value: 0

Name: wFlags
Type: Integer
Contains task flags
Do not modify

Name: wTime
Type: Integer
Contains time information when task to be launched
Do not modify

Name: wDate
Type: Integer
Contains date information when task to be launched
Do not modify

[TaskDefinition]

Name: szTaskName
Type: String
Defines task name
Default value: New Scan Task

Name: wTaskAttrib

Type: Integer
Contains task attributes
Do not modify

Name: wTaskType
Type: Integer
Contains task type
Do not modify

Alert Message variables

Alert messages generated by NetShield **may** contain following variables:

- %FILENAME% - Name of the infected file
- %TASKNAME% - Name of the task that detected the virus
- %VIRUSNAME% - Name of the virus
- %DATE% - Date of the event
- %TIME% - Time of the event

Note

- Use these variables to create custom alert messages.

To view the virus list

1 Click  or select Virus List from the Tools menu of the Console.
The Virus List appears.

2 To find out specific information about a virus, highlight the virus and click **Virus Info**.
The Virus Information properties sheet appears with information about the virus, its properties, and whether or not there is a virus remover available.

Tip

- To open the virus list, click here  .

ScanConfig

The ScanConfig properties sheet is where Scan tasks are configured.

To configure a scan task, highlight the task and click  or select Properties from the Edit menu

Acrobat Error Message

You must have Adobe Acrobat to view this file.

Safe Computing Practices

Safe computing practices include:

Virus protection
Regular backups
Meaningful password protection
Training and awareness

{button ,JI(`SHIELD.HLP',`Books_on_virus_protection_and_security')} Related Topics

Inbound Files

Inbound Files are files copied to the server.

Outbound Files

Outbound Files are files copied from the server.

Removing a Notification Item

To remove an alert notification item, highlight the item and click **Remove**.

Viewing notification item properties

To view the properties of an alert notification item, highlight the item and click **Properties**.

To view the log file

Open the log file using any text editor.

To open the Application Log

Click  or select Event Log from the Tools menu.

To configure the modem

1 Click **Modem**. The Modem Configuration page is displayed.
2 Choose the modem brand and model from the drop down list.
3 Select the COM port.
4 Set the maximum baud rate.
5 Select any prefix required to get an outside line.
6 Select tone or pulse dialing.
7 Click **OK**

To start Scan

Double-click the Scan icon in the NetShield program group.