

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.

See also

{button ,JI(`shield.HLP',`IDH_Boot_virus')} [Boot virus](#)

{button ,JI(`shield.HLP',`IDH_File_virus')} [File virus](#)

{button ,JI(`shield.HLP',`IDH_Macro_virus')} [Macro virus](#)

{button ,JI(`shield.HLP',`IDH_Stealth_virus')} [Stealth virus](#)

{button ,JI(`shield.HLP',`IDH_Multi_partite_virus')} [Multi-partite virus](#)

{button ,JI(`shield.HLP',`IDH_Mutating_virus')} [Mutating virus](#)

{button ,JI(`shield.HLP',`IDH_Encrypted_virus')} [Encrypted virus](#)

{button ,JI(`shield.HLP',`IDH_Polymorphic_virus')} [Polymorphic virus](#)

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



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



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



A stealth virus hides itself to evade detection. It stealth virus may be a [boot virus](#) or a [file virus](#).



A multi-partite acts like a [boot virus](#) and a [file virus](#) by spreading through boot sectors and files.



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



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



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



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.

Network Associates' 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 VirusScan;What is a computer virus?',0,','')} [Related Topics](#)



Superior detection

- NCSA-certified scanner assures detection of 100% of viruses found “in the wild.” See the NCSA website, www.ncsa.com .
- VirusScan employs Hunter engine technology for pinpoint virus identification accuracy.
- On-access (inbound and outbound) scanning provides real-time identification of both known and unknown viruses upon file access, create, copy, rename, and run; disk access; system startup; and system shut down.
- On-demand scanning provides for user-initiated detection of known [boot](#), [file](#), [mutating](#), [macro](#), [stealth](#), and [encrypted](#), viruses located within files, drives, and diskettes.

Automated protection

- VirusScan can be configured for an automated response on virus detection including notification, logging, deletion, isolation, or cleaning
- Supports Windows NT services and file system
- Flexible scheduling and immediate scanning options

Administrative ease

- Advanced alerting features include alphanumeric pager, e-mail via SMTP, SNMP, DMI, and NT event logging
- Centralized alerting and reporting from workstations
- Scan Wizard assists users in creating new scan tasks
- AutoUpdate feature allows for immediate or scheduled updating via a central shared location or FTP download
- The Service Password command-line utility allows administrators to set or change the user ID and passwords used by McAfee Services on one or more systems
- Monthly updates of virus signatures are included with the purchase of a Network Associates subscription license to assure the best detection and removal rates.



Founded in 1989, Network Associates 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. Network Associates is also the pioneer and leading provider of electronically distributed software. All of Network Associates' products may be purchased through dealers or downloaded from bulletin board systems and on-line services around the world.

Network Associates 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 Network Associates or our network of more than 150 authorized agent offices in 50+ countries worldwide.



NetShield for Windows NT is a client-server application with the NetShield server software composing the server end of the relationship and the VirusScan client software composing the workstation end of the relationship. The NetShield server software runs in the background without any assistance. NetShield provides robust virus protection to users who access file and services on this system.



Use the AntiVirus Console to configure the [on-access task](#), [on-demand tasks](#), and [AutoUpdate tasks](#). In addition to configuring task functions, the Console can receive information such as statistics and alarm notifications.

See also

{button ,JI('shield.HLP','IDH_Tasks')} [What are tasks?](#)



Tasks are individually configured jobs which are responsible for virus protection and file updating activities. Each task appears as a separate entry in the [AntiVirus Console](#) window. There are three types of tasks: the [on-access task](#), [on-demand tasks](#), and [AutoUpdate tasks](#).

 [Related topics](#)



The on-access [task](#) monitors files copied to and from your workstation via network connections and floppy diskettes . Use this task to specify what types of files are scanned and how VirusScan responds to infected files.




On-demand [tasks](#) are drive-scanning tasks. On-demand tasks can be scheduled to automatically scan workstation drives. You may specify what files are scanned, how often a scan takes place, and how VirusScan responds to infected files.




A scheduled task is an [on-demand task](#) configured to run at times specified by you or your administrator.




- 1 Click  or select **New Task** from the Scan menu. A new scan task appears in the Console task window.
- 2 Type in a new name for the task and press ENTER. The task is created and [Task Properties](#) dialog box 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(^ Configuring an on-demand task;creating the on-access task;scheduling an on-demand task (overview)',0,'')} Related Topics



- 1 Highlight the task you want to configure in the AntiVirus Console
- 2 Click  or select Properties from the Edit menu.
The [Task Properties](#) dialog box appears with the Detection page displayed. You are ready to configure this task.

See also

{button ,JI(`shield.HLP',`IDH_Creating_an_on_demand_task')} [Creating an on-demand task](#)

{button ,JI(`shield.HLP',`IDH_Adding_files_to_scan')} [Adding files to scan](#)

{button ,JI(`shield.HLP',`IDH_Setting_how_VirusScan_responds_to_a_virus')} [Setting VirusScan's response to an infection](#)

{button ,JI(`shield.HLP',`IDH_Creating_a_virus_activity_log_file')} [Virus logging and reporting](#)

{button ,JI(`shield.HLP',`IDH_Scheduling_a_task')} [Scheduling an on-demand task](#)

{button ,JI(`shield.HLP',`IDH_Adding_a_file_or_folders_to_exclude')} [Excluding files, folders, and drives from scanning](#)



VirusScan 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

- 2 A good strategy for protecting your network is to focus highly susceptible areas (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](#)



- 1 Select the detection page from the [Task Properties](#) dialog box.
- 2 Click **Add**.
- 3 Select the files to scan.
 - To scan all local drives, select **All Local Drives**.
 - To scan specific drives and folders, select **Drive or Folder**.
 - To scan a specific file, select **File**.
- 4 Enter the path to the drive, folder , or file to scan or click **Browse** to navigate to the item. Click **OK**. The new item appears in the Detection window.
- 5 Repeat Steps 1 through 4 until all scan items are entered.
- 6 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.
- 7 To include the scanning of subfolders, check Include Subfolders.
- 8 To include scanning of compressed files, check the [Compressed Files](#) checkbox.
- 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(`ODT;FILODT',0,','')} [Related Topics](#)



- 1 Select the Detection page from the [Task Properties](#) dialog box.
- 2 Highlight an item and click **Edit**.
- 3 Select the files to scan.
 - To scan all local drives, select **All Local Drives**.
 - To scan specific drives and folders, select **Drive or Folder**.
 - To scan a specific file, select **File**.
- 4 Enter the path to the drive, folder, or file. Click **Browse** to navigate to the item.
- 6 Click **OK**. The edited item appears in the Detection window.
- 7 To further configure this task, select another properties 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(`FILODT',0,'')} [Related Topics](#)



- 1 Select the Detection page from the [Task Properties](#) dialog box.
- 2 Highlight the Scan item to delete and click **Remove**.
- 3 To add items, click [Add](#).

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



- 1 Select the Action page from the [Task Properties](#) dialog box.
- 2 Set how VirusScan responds to an infected file:

```
{button ,JI('shield.HLP',`IDH_NetShield_moves_the_infected_files_to_a_folder')} Move infected files to a folder  
{button ,JI('shield.HLP',`IDH_Continues_Scanning')} Continue scanning  
{button ,JI('shield.HLP',`IDH_Cleans_the_infected_file')} Clean infected files automatically  
{button ,JI('shield.HLP',`IDH_Deletes_the_infected_file')} Delete infected files automatically
```

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



You can configure VirusScan to respond to infected files by prompting you for action, by relocating the infected file to a quarantine folder, 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](#)



Select **Continue Scanning** to instruct VirusScan to continue with the scan without taking any action.

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



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**.

Note: If this option is selected, VirusScan changes the infected file extension to .VIR. Confirm that report logging is enabled to ensure you have a record of which files were locked so you can clean them or restore them from backups.



Select **Delete Infected File** to configure VirusScan to delete infected files as soon as it detects them. If you select this option, confirm that activity logging is enabled. This will ensure you have a record of which files were deleted, so you can restore them from backups.



Scan offers a very flexible scheduling interface which allows customization of scans to fit your 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.

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



- 1 Select the Schedule page from the [Task Properties](#) dialog box.
- 2 Check the **Enable Scheduler** checkbox.
- 3 Select the type of schedule to configure.

{button ,JI('shield.HLP','IDH_One_time_task')} [One time task](#)
{button ,JI('shield.HLP','IDH_Hourly_task')} [Hourly task](#)
{button ,JI('shield.HLP','IDH_Daily_task')} [Daily task](#)
{button ,JI('shield.HLP','IDH_Weekly_task')} [Weekly task](#)
{button ,JI('shield.HLP','IDH_Monthly_tasks')} [Monthly task](#)
{button ,JI('shield.HLP','IDH_Task_that_runs_at_Startup')} [Task that runs at system startup](#)

{button ,AL('ODT',0,'')} [Related Topics](#)



- 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**.



- 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.



- 1 Click the **Daily** radio button.
- 2 Click the **Which Days** button. The Select Days dialog box appears.
- 3 Select which day(s) the task runs (i.e. Sunday, Monday, etc.) and click **OK**.
- 4 Enter the time to start the task in the Start At field.
- 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**.



- 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**.



- 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**.



- 1 Click the **At Startup** radio button. This tells VirusScan to perform a scan every time the system is started.
- 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**.



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](#)



- 1 Select the Exclusions page from the [Task Properties](#) dialog box.
- 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](#)



- 1 Select the Exclusions page from the [Task Properties](#) dialog box.
- 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](#)



- 1 Select the Exclusions page from the [Task Properties](#) dialog box.
- 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](#)



If enabled, VirusScan 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](#)



- 1 Select the Reports page from the [Task Properties](#) dialog box.
- 2 Check the **Log to File** checkbox. The default log file location is C:\Win32app\VirusScan\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](#)



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](#)



1 Highlight the on-access task.

2 Click  or select Properties from the Edit menu.

The VirusScan Properties dialog box appears with the Detection page displayed. You are ready to configure this task.

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



When configuring the on-access task, be sure to check both [Inbound](#) and [Outbound](#) checkboxes.

Tip

§ To improve scan performance, configure VirusScan to only check specified file types which are likely to be infected (.EXE, .COM, DO?, .XL?, .SYS, .BIN, .RTF, .OBD).

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



- 1 Select the Detection page from the [VirusScan Properties](#) dialog box.
- 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 Select the **Enable On-Access Scanning at System Startup** checkbox to tell VirusScan to automatically start scanning each time the computer is started.
Note: To manually start or stop the VirusScan service, use the Services Manager located in the Control Panel. For more information, refer to the documentation that accompanied Microsoft NT. Select the **Users Are Allowed To Disable VirusScan** checkbox to allow disabling of the on-access task from the AntiVirus Console.
- 6 Select the **Enable File Scan Caching** checkbox to improve over-all on-access scanning performance of VirusScan. When this option is enabled, VirusScan will only scan files the first time they are accessed after the system or Task Manager is restarted. If a file in the cache is modified, VirusScan will rescan the file.
- 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(`OAT',0,'')} [Related Topics](#)



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

.EXE
.COM
.SYS
.DO?
.XL?
.SYS
.BIN
.ODB
.RTF

Note: It uses the extensions .DO?, and .XL? to identify Microsoft Word and Excel document and template files, which can contain macro viruses. The ? character is a wildcard.

- 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**.



VirusScan can prevent the spread of an infection by automatically cleaning, deleting, relocating or denying access to infected files.

Note

§ You may choose only one of these options.

{button ,AL(`odta;Setting how VirusScan reponds to a virus',0,','')} [Related Topics](#)



1 Select the Action page from the [VirusScan Properties](#) dialog box.

2 Select how VirusScan responds to an infected file.

{button ,JI('shield.HLP',`IDH_NetShield_cleans_the_infected_files')} [Cleans the infected files](#)

{button ,JI('shield.HLP',`IDH_NetShield_deletes_the_infected_files')} [Deletes the infected files](#)

{button ,JI('shield.HLP',`IDH_NetShield_moves_the_infected_files_to_a_folder')} [Moves the infected files to a folder](#)

{button ,JI('shield.HLP',`IDH_NetShield_denies_access_to_the_infected_files')} [Denies access to the infected files](#)

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



Select this option to clean infected files automatically. If a virus cannot be removed from a file or the file is damaged beyond repair, VirusScan automatically denies access to the file. If this occurs, delete the file and restore the original from backups.

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



Choose this option to tell VirusScan to delete infected files as soon as it detects them. If you select this option, confirm that activity logging is enabled. This will ensure you have a record of which files were deleted, so you can restore them from backups.

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



Select this option to tell VirusScan to move infected files to a “quarantine” folder. Enter the name of the quarantine folder that will receive forwarded messages in the Folder To Move To text box. You can enter the folder name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the folder on the network.

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



This option is recommend for systems left unattended. If this option is selected, VirusScan denies user access to the infected files existing on the workstation and appends infected files written to the workstation with a .VIR extension.

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

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



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

Tip

§ If you set VirusScan 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](#)



- 1 Select the Exclusions page from the [VirusScan Properties](#) dialog box.
- 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](#)



- 1 Select the Exclusions page from the [VirusScan Properties](#) dialog box.
- 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](#)



- 1 Select the Exclusions page from the [VirusScan Properties](#) dialog box.
- 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](#)



If enabled, VirusScan 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](#)



- 1 Select the Reports page from the [VirusScan Properties](#) dialog box.
- 2 Check the **Log to File** checkbox. The default log file location is C:\Program Files\McAfee\VirusScan\VirusScanActivityLog.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](#)



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

- 1 Select the Detection page from the [VirusScan Properties](#) dialog box.
- 2 Check the **Enable On-access Scanning at System Startup** checkbox.



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 **Users are Allowed to Disable VirusScan** checkbox.



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.



To quickly configure multiple computers and save time, VirusScan 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 [Task Properties](#) dialog box 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](#)



- 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](#)




Network Associates' AutoUpdate program is a powerful updating utility that can ensure you have the latest VirusScan files installed. AutoUpdate can automatically retrieve the latest VirusScan files from Network Associates' FTP site or a local network computer and overwrite old VirusScan files on your network. Use the AutoUpdate tasks to automate and customize the updating process.

Network Associates offers two AutoUpdate tasks to keep your VirusScan files up-to-date:

{button ,JI('shield.HLP','Automatic_DAT_Update_task')}Automatic DAT Update

{button ,JI('shield.HLP','Automatic_Product_Upgrade_task')}Automatic Product Upgrade

Both AutoUpdate tasks appear in the Console task window preceded by .




Related topics



New viruses are discovered at a rate of more than 200 a month. Often, these viruses are not detected using older versions of virus detection products or virus signature (DAT) files. The DAT files that came with your copy of VirusScan may not detect a virus that was discovered after you bought the product. As new viruses are discovered, Network Associates updates these data files to detect new viruses on a monthly basis. Network Associates recommends that you update your data files and product on a regular basis to prevent infection from new viruses.

To update your VirusScan files regularly and conveniently, use any of the following methods:

AutoUpdate. Use Network Associates' automatic update utility to update your files automatically and invisibly. To learn more, click [here](#) 

Network Associates electronic services. Connect to any of the electronic services, including the Network Associates Web Site and Network Associates BBS to update your files.

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



- 1 Select AutoUpdate from the Tools menu. The AutoUpdate dialog box appears with the Update Options page appears.
- 2 Click the **Copy from a Local Network Computer** radio button. Then enter the name of the computer that AutoUpdate will copy the files from in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the computer on the network.
- 3 To perform the update now, click **Update Now**.
- 4 To schedule this script, click the [Schedule](#) tab.

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



- 1 Select AutoUpdate from the Tools menu.
- 2 Configure the AutoUpdate options on the Update Options or Upgrade Options page.
- 3 Click the Schedule button.
- 4 Check the **Enable Scheduler** checkbox.
- 5 Determine how often the AutoUpdate task will run.
 - {button ,JI('shield.HLP',`IDH_To_schedule_a_one_time_update'`} [One time update](#)
 - {button ,JI('shield.HLP',`IDH_To_schedule_a_hourly_update'`} [Hourly update](#)
 - {button ,JI('shield.HLP',`IDH_To_schedule_a_daily_update'`} [Daily update](#)
 - {button ,JI('shield.HLP',`IDH_To_schedule_a_weekly_update'`} [Weekly update](#)
 - {button ,JI('shield.HLP',`IDH_To_schedule_a_monthly_update'`} [Monthly update](#)
 - {button ,JI('shield.HLP',`IDH_To_schedule_an_update_that_runs_transparently_at_Startup'`} [Update that runs at system startup](#)

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



- 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](#)



- 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](#)



- 1 Click the **Daily** radio button.
- 2 Click the Which Days button. The Select Days dialog box appears.
- 3 Select which day(s) the update runs (ie: Sunday, Monday, etc.) and click **OK**.
- 4 Enter the time to start the task in the Start At field.
- 5 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](#)



- 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](#)



- 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](#)



- 1 Click the **At Startup** radio button. This tells AutoUpdate to download VirusScan files every time the Network Associates service is started.
- 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](#)



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](#)



Approximately once a month, Network Associates updates VirusScan 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','IDH_McAfee_bulletin_board_system__BBS_')} [Network Associates bulletin board system \(BBS\)](#)

{button ,JI('shield.HLP','IDH_McAfee_Forum_on_CompuServe')} [Network Associates Forum on CompuServe](#)

{button ,JI('shield.HLP','IDH_Internet_Access')} [Internet Access](#)



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 Network Associates BBS phone number is (408) 988-4004.



We sponsor the Network Associates 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.



The latest versions of Network Associates' anti-virus software are available by anonymous ftp (file transfer protocol) over the Internet from the site [ftp.mcafee.com](ftp://ftp.mcafee.com). 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.

Network Associates' 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](ftp://wuarchive.wustl.edu) (US).

[ftp.switch.ch](ftp://ftp.switch.ch) (Switzerland).

[ftp.funet.fi](ftp://ftp.funet.fi) (Finland).

[src.doc.ic.ac](ftp://src.doc.ic.ac) (UK).

[archie.au](ftp://archie.au) (Australia).



Although VirusScan is designed to offer the highest degree of virus protection, detection and eradication available, no anti-virus program can stop 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](#)



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](#)



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

To administer VirusScan from Windows 95:

- 1 Install the VirusScan Console. See the VirusScan User's Manual.
- 2 Select the Console icon in the VirusScan Group.
- 3 When prompted, enter the system to administer or click **Browse**.



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

{button ,JI(`shield.HLP',`IDH_Virus_found__Clean_infected_file')} Clean infected file
{button ,JI(`shield.HLP',`IDH_Virus_found__Delete_infected_file')} Delete infected file
{button ,JI(`shield.HLP',`IDH_Virus_found__Move_infected_file_to_a_folder')} Move infected file to a folder
{button ,JI(`shield.HLP',`IDH_Virus_found__Continue_scanning')} Continue scanning



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

Tips

- § To customize notification methods, see [Overview: Alert Manager](#).
- § To learn more about your virus, see the [Virus Information Library](#) .



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

n To learn more about your virus, see the [Virus Information Library](#) .



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 [Network Associates' Virus Information Library](#).



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 [Network Associates' Virus Information Library](#) .



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, VirusScan ignores any viruses encountered.

Tip

n To learn more about your virus, see [Network Associates' Virus Information Library](#) .



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 Emergency Recovery diskette.

Tip

n To learn more about your virus, see [Network Associates' Virus Information Library](#) .



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

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

§ Confirm VirusScan 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, VirusScan 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.



- § 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 Network Associates 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



Usage

SCAN32 [<switches>] [<scanitem>]

SCAN32 <config.VSC> [<override_switches>] [<override_scanitem>]

SCAN32 [/SERVER <servername>] /TASK <taskid> [<override_switches>] [<override_scanitem>]

/[NO]SPLASH Default: ***/SPLASH***

/[NO]AUTOSCAN

Displays initial splash screen.

Scan32 automatically initiates scanning when started.

Default: <depends on UI type>

/[NO]AUTOEXIT

Scan32 automatically exits if no viruses are found. If viruses are found, Scan32 does not exit (see ***/ALWAYSEXIT***).

Default: <depends on UI type>

/[NO]ALWAYSEXIT

Scan32 automatically exits when scan is complete. Scan32 exits even if viruses are detected (see ***/AUTOEXIT***).

Default: <depends on UI type>

/[NO]SUB

Use this switch to scan all subfolders.

Default: ***/SUB***

/[NO]ALL

Scans all files, regardless of their file extension.

Default: ***/NOALL***

/[NO]COMP

Scans compressed files and ZIP files.

Default: ***/COMP***

/UICONFIG | /UIEXONLY | /UINONE

Specifies the type of graphical user interface displayed:

Default: ***/UICONFIG***

- ***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>

Specifies what action to take when a virus is detected:

Default: ***/CONTINUE***

- ***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.



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

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



- 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](#)



1 Select the Actions page from the [Scan](#) properties sheet.

2 Set how Scan responds to an infected file:

{button ,JI('shield.HLP',`IDH_Scan__prompts_you_for_Action')} [Prompts you for action](#)

{button ,JI('shield.HLP',`IDH_Scan__continues_without_taking_any_action')} [Continues scanning without taking any action](#)

{button ,JI('shield.HLP',`IDH_Scan__moves_infected_files_to_a_folder')} [Automatically moves infected files to a folder](#)

{button ,JI('shield.HLP',`IDH_Scan__automatically_cleans_infected_files')} [Automatically cleans infected files](#)

{button ,JI('shield.HLP',`IDH_Scan__automatically_deletes_infected_files')} [Automatically deletes infected files](#)

Note: You may only choose one of these options.

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



- 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.



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, VirusScan ignores any viruses encountered.



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.



- 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.



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

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



- 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\VirusScan\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](#)



The VSC file is a configuration text file, formatted similarly to the Windows INI file, which outlines VirusScan's settings. Each variable in the file has a name followed by the equal (=) sign and a value. The values define which settings were selected for the configuration.

The variables are arranged in five groups: ScanOptions, AlertOptions, ActivityLogOptions, Scheduler, and TaskDefinitions. To edit the VSC file, right-click the filename and select Edit.

ScanOptions

SzProgramExtensions	<i>Type: String</i> <i>Defines extensions to be used as program extensions during scan</i> <i>Default value: EXE COM DLL SYS DO?</i>
SzDefaultProgramExtensions	<i>Type: String</i> <i>Defines extensions to be used as default program extensions during scan configuration</i> <i>Default value: EXE COM SYS DO? XL? BIN RTF OBD</i>
BIncludeSubFolders	<i>Type: Boolean (1/0)</i> <i>Instructs scanner to search for viruses inside subfolders</i> <i>Default value: 1</i>
BScanAllFiles	<i>Type: Boolean (1/0)</i> <i>Instructs program to scan inside all files</i> <i>Default value: 0</i>
bScanCompressed	<i>Type: Boolean (1/0)</i> <i>Instructs program to scan inside compressed files (PkLite, LHA, LZEXE, ZIP, Microsoft CAB)</i> <i>Default value: 1</i>
uScanAction	<i>Type: Integer (1-5)</i> <i>Defines what action will be taken upon virus detection:</i> <i>1 - Prompt for Action</i> <i>2 - Continue Scanning</i> <i>3 - Move Infected File</i> <i>4 - Clean Infected File</i> <i>5 - Delete Infected File</i> <i>Default value: 1</i>
BautoStart	<i>Type: Boolean (1/0)</i> <i>Defines if scan will be started immediately upon launch</i> <i>Default value: 0</i>
BAutoExit	<i>Type: Boolean (1/0)</i> <i>Defines if scanner will be unloaded when scan is finished</i> <i>Default value: 0</i>

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

AlertOptions

BDisplayMessage Type: Boolean (1/0) Defines if custom message should be displayed upon virus detection Default value: 1
SzCustomMessage Type: String Defines custom message to be displayed upon virus detection Default value: Your custom message here!
BSoundAlert Type: Boolean (1/0) Defines if audible alert should be made upon virus detection Default value: 1

ActivityLogOptions

BLogToFile Type: Boolean (1/0)
Defines if scan results should be logged into log file
Default value: 1
BLimitSize Type: Boolean (1/0)
) Defines if size of the log file should be limited
Default value: 1
uMaxKilobytes Type: Integer
Defines maximum size of the logfile
Default value: 100
SzLogFileName Type: String
Defines log file name
Default value: VirusScanActivity Log.txt
BLogDetection Type: Boolean (1/0)
Defines if scan results should be logged
Default value: 1
BLogClean Type: Boolean (1/0)
Defines if clean results should be logged
Default value: 1
BLogDelete Type: Boolean (1/0)
Defines if infected file delete operations should be logged.
Default value: 1

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

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

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

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

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

TaskDefinition

SzTaskName Type: String
Defines task name
Default value: New Scan Task

WTaskAttrib Type: Integer
Contains task attributes
Do not modify

WTaskType Type: Integer
Contains task type
Do not modify

Scheduler

BSchedEnabled Type: Boolean (1/0)
Enables scheduling for the task.
Default value: 0

WFlags Type: Integer
Contains task flags.
Do not modify.

WTime Type: Integer
Defines time when task is to be launched.
Do not modify.

WDate Type: Integer

*Defines date when task is to be launched.
Do not modify.*



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


Variable	Description
%FILENAME%	<i>Name of the infected file</i>
%TASKNAME%	<i>Name of the task that detected the virus</i>
%VIRUSNAME%	<i>Name of the virus</i>
%DATE%	<i>Date of the event</i>
%TIME%	<i>Time of the event</i>
%COMPUTERNAME%	<i>Name of the infected computer</i>
%SOFTWARENAME%	<i>Name of the software that detected the virus</i>
%SOFTWAREVERSION%	<i>Version number of the software that detected the virus</i>

Note: Use these variables to create [custom alert messages](#).



Task Properties Dialog Box

The Task Properties dialog box is where on-demand scan tasks are configured.

To configure an on-demand 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 include:

- n Virus protection
- n Regular backups
- n Meaningful password protection
- n Training and awareness



Inbound Files

Inbound Files are files copied to the workstation.

Outbound Files

Outbound Files are files copied from the workstation.

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 VirusScan

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

Macro viruses infect Microsoft Word and Excel files by using their embedded macro functionality. Microsoft incorporated macro functionality into their Word and Excel products to automate repetitive tasks and combine multiple commands. Although the intentions were good, it was eventually discovered that macros could be used for nefarious purposes.



To start the AntiVirus Console, do one of the following:


- In Windows NT 3.51, open the VirusScan group in the Program Manager, and double-click the AntiVirus Console icon .
- In Windows NT 4.0, click Start, select VirusScan in the Programs menu, and select AntiVirus Console.



The AutoUpdate tasks automatically download updates and upgrades from an FTP site or network distribution site. After the VirusScan files are downloaded, AutoUpdate can either post them to a distribution site for downloading by other computers or automatically apply the new files to your VirusScan machines.

Use the AutoUpdate tasks to automate and customize the updating process. Network Associates offers two AutoUpdate tasks to keep your VirusScan files up-to-date:

- [Automatic DAT Update task](#)
- [Automatic Product Upgrade](#)

Both tasks appear in the AntiVirus Console task window preceded by  .

See also

{button ,JI('shield.HLP',`IDH_To_configure_an_Automatic_DAT_Update_task')} [Configuring the Automatic DAT Update task](#)

{button ,JI('shield.HLP',`IDH_Configuring_Automatic_Program_Upgrade_task')} [Configuring the Automatic Program Upgrade task](#)



The files CLEAN.DAT, NAMES.DAT, SCAN.DAT, and MCALYZE.DAT all provide virus information to the VirusScan software and make up the VirusScan virus signature (DAT) files.

Network Associates updates the DAT files approximately once a month with new virus detectors, cleaners, and fixes to reported bugs.

Network Associates upgrades the VirusScan program periodically with new features, enhancements, and functionality to provide you with the latest antivirus technology.



Use the AutoUpdate Properties dialog box to configure an Automatic DAT Update task.

- 1 Select AutoUpdate from the Tools menu.
- 2 Click the Update Options tab.
- 3 Select the transfer method in which you want to receive the files. Your options are:
 - [Copy from Local Computer.](#)
 - [FTP from a Remote Network computer.](#)
- 4 Click the FTP Login Information button to enter your FTP access information, such as username and password or select the Use Anonymous FTP Login checkbox. If this option is selected, AutoUpdate will automatically assign “Anonymous” as your user name and assign your e-mail address as your password.

Note: Use anonymous when connecting to Network Associates’ FTP site.

- 5 Select the Use Proxy Server checkbox if your network uses a proxy server or gateway to direct ftp commands. Enter the name and port number of the proxy server. If you are unsure if your network uses a proxy server or if you do not know the port number, check with your system administrator.
- 6 Select the Log Activity into the [VirusScan Activity Log File](#) checkbox to record the AutoUpdate history.
- 7 To update the DAT files now, click the Update Now button.
- 8 To perform scheduled DAT file updates, click the [Schedule](#) button.
- 9 Click the [Advanced](#) button to configure AutoUpdate to perform special actions during or after the updating process.

See also

{button ,JI(`shield.HLP',`IDH_Scheduling_AutoUpdates')} [Scheduling AutoUpdate tasks](#)

{button ,JI(`shield.HLP',`Additional_updating_options')} [Additional AutoUpdate options](#)

{button ,JI(`shield.HLP',`IDH_Configuring_Automatic_Program_Upgrade_task')} [Configuring the Automatic Product Upgrade task](#)



The AutoUpdate tasks and can also perform services during and after the updating process. You can configure the AutoUpdate tasks to automatically:

```
{button ,JI('shield.HLP','IDH_Backup_existing_DAT_files')} Backup existing VirusScan files  
{button ,JI('shield.HLP','IDH_Retrieve_the_update_but_do_perform_the_update')} Retrieve the updated VirusScan files without performing the update  
{button ,JI('shield.HLP','IDH_Save_the_update_file_for_later_use_')} Save the update for later use  
{button ,JI('shield.HLP','IDH_Run_a_program_after_updating_')} Run a program after updating the VirusScan files
```



To back up existing VirusScan files automatically, click the Advanced button on the Update Options property page. Then, select the **Backup the Existing DAT Files** checkbox.



To retrieve the updated files without performing the update, click the Advanced button on the Update Options property page. Then, select the **Retrieve the Update File but do Not Perform the Update** checkbox to save new files on your workstation without applying them. Click **OK**.

Note: If this option is selected, you must select the **Save the Update for Later Use** checkbox and specify the location in which the file can be retrieved.



After retrieving an update, AutoUpdate can store the update module in a location accessible by all computers running VirusScan for Windows NT. To configure AutoUpdate to store update modules for distribution, click the **Advanced** button on the Update Options property page. Then, select the **Save the Update File for Later Use** checkbox to save the new DAT files in special location. Enter a location in which you want to store the update. Click **OK**.




To run a program after AutoUpdate retrieves the update, click the **Advanced** button on the Update Options property page. Then, select the **Run a Program After a Successful Update** checkbox to automatically execute a program or script upon downloading the update. Enter the complete path to the file that will be run or click Browse to navigate to the program. Click **OK**.




Compressed file scanning option

Select this option if you want VirusScan to scan files compressed with PKLITE, LZEXE, LHA, WinZip, Microsoft CAB.

The VirusScan Properties dialog box is where on-access scan tasks are configured.

To configure an on-access scan task, highlight the task and click  or select Properties from the Edit menu.



The Task Properties dialog box is where VirusScan tasks are configured. To configure a scan task, highlight the task and click  or select Properties from the Edit menu.



Copy from local computer

Choose this option to copy files from a designated local computer. Then enter the name of the computer that AutoUpdate will copy the files from in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the computer on the network.

FTP from a remote network computer

Choose this option to download files from a designated network computer. Then Enter the FTP computer name and directory in which the files will be downloaded from. The default FTP computer name and directory is `ftp.web.mcafee.com/pub/antivirus/datafiles/3.x`.

VirusScan Activity Log File

The VirusScan Activity Log File lists the each step made by AutoUpdate during the updating process. The log file will also include a specific error message if any of these steps fail.

To configure the Automatic Product Upgrade task to acquire the most current version of VirusScan, follow these steps:

- 1 Select AutoUpdate from the Tools menu.
- 2 Click the Upgrade Options tab.
- 3 Select the transfer method in which you want to receive the files. Your options are:
[Copy from Local Computer](#)
[FTP from a Remote Network computer.](#)
- 4 Click the FTP Login Information button to enter your FTP access information, such as username and password or select the Use Anonymous FTP Login checkbox. If this option is selected, AutoUpdate will automatically assign “Anonymous” as your user name and assign your e-mail address as your password.

Note: Use anonymous when connecting to Network Associates’ FTP site.

- 5 Select the Use Proxy Server checkbox if your network uses a proxy server or gateway to direct ftp commands. Enter the name and port number of the proxy server. If you are unsure if your network uses a proxy server or if you do not know the port number, check with your system administrator.
- 6 Select the Log Activity into the [VirusScan Activity Log File](#) checkbox to record the AutoUpdate history.
- 7 To upgrade VirusScan now, click the Upgrade Now button.
- 8 To perform scheduled upgrades, click the [Schedule](#) button.
- 9 Click the [Advanced](#) button to configure AutoUpdate to perform special actions during or after the updating process.



Automatic DAT Update task

Create an Automatic DAT Update task to automatically retrieve and install DAT files.

Automatic Product Upgrade task

Create an Automatic Product Upgrade task to automatically retrieve and install the latest VirusScan program files.

Scan compressed files

VirusScan's on-access scanner can scan files compressed with PKLITE and LZEXE.

To configure VirusScan to send a disconnect message to the infected computer, select the Send Message to User checkbox and enter a custom message in the text box provided.



Network Associates maintains a support staff with expertise in the each of the areas listed below. Click any of these topics for more information:

{button ,JI('shield.HLP','McAfee_Training')} [Network Associates training](#)

{button ,JI('shield.HLP','Technical_Support')} [Technical support](#)



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

McAfee, Inc.
2805 Bowers Avenue
Santa Clara, CA 95051-0963
U.S.A.

[See also](#)

[{button ,JI\(`shield.HLP',`McAfee_Training'\)} Network Associates training](#)

[{button ,JI\(`shield.HLP',`Technical_Support'\)} Technical Support](#)



To learn about scheduling on-site training for any Network Associates product, call (800) 338-8754.

See also

{button ,JI(`shield.HLP`,`Customer_Care`)} [Customer Care](#)

{button ,JI(`shield.HLP`,`Technical_Support`)} [Technical Support](#)



Network Associates is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web a valuable resource for answers to technical support issues. We encourage you to make this your first stop for answers to frequently asked questions, for updates to Network Associates software, and for the latest news and information. Click the website address shown below to link directly to Network Associates' site.

World Wide Web <http://www.networkassociates.com>
Click [here](#) to link to the Network
Associates Web Site.

If you do not find what you need or do not have Web access, try one of Network Associates' automated services:

**Automated Voice and Fax
Response System** (408) 988-3034

E-mail support@mcafee.com

**Network Associates dial-up
Bulletin Board System** (408) 988-4004
1200 bps to 28,800 bps
8 bits, no parity, 1 stop bit
24 hours, 365 days a year

CompuServe GO MCAFEE

America Online Keyword MCAFEE

If the automated services do not have the answer you need, contact Network Associates at one of the following numbers Monday through Friday between 6:00 a.m. and 6:00 p.m. Pacific time.

For corporate-licensed customers:

Phone (408) 988-3832

Fax (408) 970-9727

For retail-licensed customers:

Phone (972) 278-6100

Fax (408) 970-9727

To provide the answers you need quickly and efficiently, the Network Associates technical support staff needs some information about your computer and software. Please have this information ready before you call:

- Product name and version number
- Computer brand and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers
- Network type and software version numbers
- Contents of your AUTOEXEC.BAT file, your CONFIG.SYS file, and your system LOGIN script
- Specific steps to reproduce the problem, if applicable

See also

{button ,JI('shield.HLP','Customer_Care')} [Customer Care](#)

{button ,JI('shield.HLP','McAfee_Training')} [Network Associates training](#)



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

The Virus Information Library is available through the Network Associates Web Site.

The Virus Information Library is continuously updated to offer the most comprehensive, up-to-date information available.



%!Internet("http://www.nai.com" [here](http://www.nai.com)to go to the Virus Information Library.



Double-click an alert message to change the priority of the alert or to modify the alert message text that appears in the event log.

Alert messages generated by VirusScan **may** contain the following variables:

Variable	Description
<i>%FILENAME%</i>	<i>Name of the infected file</i>
<i>%TASKNAME%</i>	<i>Name of the task that detected the virus</i>
<i>%VIRUSNAME%</i>	<i>Name of the virus</i>
<i>%DATE%</i>	<i>Date of the event</i>
<i>%TIME%</i>	<i>Time of the event</i>
<i>%COMPUTERNAME%</i>	<i>Name of the infected computer</i>
<i>%SOFTWARENAME%</i>	<i>Name of the software that detected the virus</i>
<i>%SOFTWAREVERSION%</i>	<i>Version number of the software that detected the virus</i>

Note: Use these variables to create custom alert messages.

Adds a notification alert recipient.

Enter the modem's maximum baud rate.

Opens the Browse dialog box where you can select a computer.

Opens the Browse dialog box where you can select a printer to receive notifications.

Enter the amount of time between dialing the phone number and sending the message.

No help topic is associated with this item.

No help topic is associated with this item.

Lists currently configured alert recipients.

Enter any prefix required to get an outside line (eg: 9).

Selects Pulse dialing.

Enter any necessary suffix (eg: password).

Selects Tone dialing.

Enables SNMP. For more information on SNMP, refer to the operating system user's manual.

Enter the name of the email message sender.

Enter the pager ID.

Enter the Login name for the server.

Enter the message to send on detection of a virus.

Opens the Modem Settings dialog box where you can configure the modem.

Enter the modem brand and model. If your modem is not listed, select a generic modem.

Enter the pager password (if applicable).

Enter the COM port where the modem is attached.

Sets the priority level for the selected alert notification. To set the alert for low, medium, and high priority alerts, select Low. To set the alert for medium and high priority alerts, select Medium. To set the alert for high priority alerts only, select High.

Displays the properties for the selected alert notification item.

Select the type of pager to receive notifications (alphanumeric or numeric).

Enter the e-mail address of the message recipient.

Removes the selected alert notification item.

Enter the amount of time between dialing the phone number and sending the message.

Enter the name of the server.

Enter the pager ID.

Enter a custom message.

Opens the SMTP (Simple Mail Transfer Protocol) configuration dialog box.

Configures SNMP. Refer to Windows NT documentation for more information.

Enter the pager password (if applicable).

Turns the modem speaker off.

Enter the amount of time between dialing the phone number and sending the message.

Sets the priority level for the selected alert notification. To set the alert for low, medium, and high priority alerts, select Low. To set the alert for medium and high priority alerts, select Medium. To set the alert for high priority alerts only, select High.

Enter an E-mail Subject line.

Tests the alert notification.

When selected, the pager receives the default alert message.

When selected, the pager receives the custom message shown below.

Enter the maximum number of characters that can be sent to the pager.

Select the modem parity settings.

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

1 Click Add.

2 Select the type of pager:

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

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

n To send pager notifications, a modem must be installed in the NetShield server. If the server does not have a modem, send a Forward to a modem-equipped NetShield server.



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 option button.
- 3 To use a custom message, click the Use custom alert message option button and enter a message in the following field.
- 4 To configure the modem settings, click Modem.
- 5 To test the pager, click Test.
- 6 To set the [priority level](#) of alert notifications this pager receives, click Priority Level.
- 7 Click OK.
- 8 To add another pager to receive notifications, click Add.
- 9 To configure other notification options, select another property page. To save the changes and exit, click OK. To cancel any changes, click Cancel.



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 To configure the modem settings, click Modem.
- 5 To test the pager, click Test.
- 6 To set the [priority level](#) of alert notifications this pager receives, click Priority Level.
- 7 Click OK.
- 8 To add another pager to receive notifications, click Add.
- 9 To configure other notification options, select another property page. To save the changes and exit, click OK. To cancel any changes, click Cancel.



Enter the server name as an Internet Protocol (IP) address, as a name your local domain name server can recognize, or in Universal Naming Convention (UNC) notation. Click OK to save your changes and return to the E-Mail Properties dialog box.

This page lists all alert notification items. To view the properties of an alert notification item, select the item and click Properties. To remove an alert notification item, select the item and click Remove.

To configure priority settings for the selected alert, drag the slider to the right to send the destination computer fewer, but higher priority, messages. Drag the slider to the left to send the destination computer more alert messages, including lower priority messages.



Alert Manager can send the alert messages that NetShield generates to other computers on your network using a standard Windows NT network message. The alert message appears on the destination computer's screen and requires the recipient to acknowledge it.

To send alerts via network messages, your NetShield server must have the Alerter and Messenger Windows NT services running. The destination computers running Windows NT must have the Messenger service running to receive alert messages. Those running Windows 95 or Windows 3.1x must also be running the WinPopup utility to receive network messages. WinPopup comes with some Windows versions. See your Windows documentation for details.

Use the Network Message property page to send alert notifications via network messages and follow these steps:

- 1 Open the Alert Manager Properties dialog box.
- 2 Click the Network Message tab.
- 3 To update this list, you can:
 - Remove a listed computer. Select one of the destination computers listed, then click Remove.
 - Add a computer to the list. Click Add to open the Network Message Properties dialog box (Figure 7-7), then enter the name of the destination computer in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the computer on the network. To choose additional options, continue with Step 4.
 - Change configuration options. Select one of the destination computers listed, then click Properties. Alert Manager opens the Network Message Properties dialog box (Figure 7-7). Change any of the information you want to change in the Computer text box, then continue with Step 4 to learn how to choose new or different configuration options.
- 4 Click [Priority Level](#) to specify which types of alert messages the destination computer will receive.
- 5 Click OK to save your changes and return to the Network Message Properties dialog box.
- 6 Click Test to send the destination computer a test message. The message will appear instantly on the destination computer's screen and the recipient will need to click OK to acknowledge it. If your recipient does not receive the message, check the Windows NT Event Viewer for an error message.



Alert Manager and [DMI](#) work together to alert the DMI management console instantly of a virus infection. When a virus is detected, DMI immediately generates an alert message for Alert Manager to display on the DMI management console.

Use the DMI property page to generate DMI alert notifications and follow these steps:

Open the Alert Manager Properties dialog box.

- 1 Click the DMI tab.
- 2 Click the Enable DMI Usage checkbox. Enable this option on the NetShield servers.
- 3 Click [Priority Level](#) to specify which types of alert messages the destination computer will receive.
- 4 Click OK to save your changes and return to the DMI dialog box.



DMI (Desktop Management Interface) is an industry interface for keeping track of and monitoring the status of components, including hardware and software, in the computers on your network. For more information about DMI, refer to your Intel documentation or visit the Desktop Management Task Force website at <http://www.dmtf.org>.

Alert Manager can be configured to launch any program or batch file on alert. For example, if your company is using cc:Mail or a special mail package that is not recognized by Network Associates, you could write a batch file to send notifications to your mail package.

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

To configure NetShield to execute a program on alert, follow these steps:

- 1 Open the Alert Manager Properties dialog box.
- 2 Click the Execute Program checkbox.
- 3 Enter the name and path of the program you want NetShield to run upon detecting a virus. You can enter the program name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the program on the network.
- 4 To execute the program on the first alert event only, click the First Time option button. To execute the program every time an alert event occurs, click the Every Time option button.
- 5 Click [Priority Level](#) to specify which types of alert messages the destination computer will receive.



Alert Manager can log the alert messages that NetShield generates to other computers on your network in a standard Windows NT Event Log. The alert message appears on the destination computer's event log and requires the recipient to acknowledge it.

To configure Alert Manager's Logging options, follow these steps:

- 1 Open the Alert Manager Properties dialog box.
- 2 Click the Logging tab. The Recipient list displays a list of all of the computers you have chosen to receive alert logging. If you have not yet chosen any destination computers, this list will be blank.
- 3 To update this list, you can:
 - Remove a listed computer. Select one of the destination computers listed, then click Remove.
 - Add a computer to the list. Click Add to open the Logging dialog box, then enter the name of the destination computer in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the computer on the network.
 - Change configuration options. Select one of the destination computers listed, then click Properties. Alert Manager opens the Logging Properties dialog box. Change any of the information you want to change in the Computer text box. Enter the computer to receive network messages or click Browse to locate the computer.
- 4 Click [Priority Level](#) to specify which types of alert messages the destination computer will receive.



Alert Manager can use .WAV files to sound an audible alert on your system when NetShield detects a virus. To use this option, your system must have a sound card.

To configure Alert Manager's Sound options, follow these steps:

- 1 Open the Alert Manager Properties dialog box.
- 2 Click the Sound tab.
- 3 Click the Enable Audible Alerts checkbox.
- 4 In the text box provided, enter the name of the sound file you want Alert Manager to run when NetShield detects a virus. The sound file must have a .WAV extension. You can enter the file name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the file on your computer.
- 5 Leave the text box blank to use the default system sound when NetShield detects a virus.
- 6 Click [Priority Level](#) to specify which types of alert messages the destination computer will receive.



In addition to automatically responding to viruses (cleaning, deleting, moving, etc.), NetShield may be configured to run a program on alert, maintain information in an event log, and alert personnel by:

[forwarding alert messages](#)

[printing alert messages](#)

[e-mailing alert messages](#)

[generating DMI alerts](#)

[sending alerts messages to a pager](#)

[SNMP](#)

[broadcasting network messages](#)

[audible alerting](#)

[Centralized Alerting](#)

[logging alert messages](#)

NetShield supports the use of any combination of notification methods and multiples of each.



NetShield uses Network Associates' Alert Manager utility to notify you or others when it detects a virus or malicious code in files on your servers. Alert Manager gives you a wide variety of notification options that you can use individually or in combinations that suit your needs.

If you have Alert Manager installed on other computers on your network, you can also forward alert messages to computers in other domains, which can in turn notify the workstations that they host about infected files on your server.

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.



Alert Manager can forward the alert messages that NetShield generates to other computers on your network. If you have installed Alert Manager on each of the destination computers, they can in turn forward alert messages to the recipients listed in their Alert Manager Summary pages. You might use this feature to pass alert messages across network domains or to construct a hierarchical arrangement for passing alert messages.

To configure Alert Manager's Forwarding options, follow these steps:

- 1 Open the Alert Manager Properties dialog box.
- 2 Click the Forward tab. The Forward page appears with a list of all of the computers you have chosen to receive forwarded messages. If you have not yet chosen any destination computers, this list will be blank.
- 3 To update this list, you can:
 - § [Remove a listed computer](#)
 - § [Add a computer to the list](#)
 - § [Change configuration options](#)
- 4 Click [Priority Level](#) to specify which types of alert messages the destination computer will receive.
- 5 Click Test to send the destination computer a test message. The message will appear instantly on the destination computer's screen and the recipient will need to click OK to acknowledge it. If your recipient does not receive the message, check the Windows NT Event Viewer for an error message.
- 6 Click OK to return to the Alert Manager dialog box.

Note

- n NetShield must be installed and running on the server receiving forwarded messages.



Select one of the destination computers listed, then click Remove.

Click Add to open the Forward Properties dialog box, then enter the name of the computer that will receive forwarded messages in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the computer on the network.

Select one of the destination computers listed, then click Properties. Alert Manager opens the Forward Properties dialog box. Change any of the information you want to change in the Computer text.

The Alert Manager supports the sending of SNMP traps. To enable SNMP, complete the following procedure:

- 1 Select the Enable SNMP checkbox.
- 2 To configure SNMP services, click Configure. The Microsoft NT Network Settings property sheet is displayed.
- 3 To complete configuration of SNMP services, refer to the network operating system documentation.
- 4 To configure other notification options, select another property page. To save the changes and exit, click OK. To cancel any changes, click Cancel.



The Alert Manager supports the sending of email messages. To send alert notifications via email, complete the following procedure:

- 1 Click Add.
- 2 Enter an email address, fill out the Subject line, and fill out the From line.
- 3 To configure SMTP settings, click Configure SMTP and enter the name of the Server and Login.
- 4 To test the connection, click Test. The message recipient receives a test message.
- 5 To set the [priority level](#) of the messages this email address receives, click Priority Level.
- 6 Click OK. To add another recipient to receive alert notifications, repeat steps 1 through 5.

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



To configure modem settings, complete the following procedure.

- 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.



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

- 1 Click Add.
- 2 Click Browse to locate the printer.
- 3 To test the connection, click Test. The printer prints a test message.
- 4 To set the [priority level](#) of the messages this printer receives, click Priority Level.
- 5 Click OK.
- 6 To add another printer to receive alert notifications, repeat steps 1 through 5.
- 7 To configure other notification options, select another property page. To save the changes and exit, click OK. To cancel any changes, click Cancel.

Note

- n Prior to configuring this notification option, the printer must be configured.



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

1 Click Add.

2 Select the type of pager:

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

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

Note

- n To send pager notifications, a modem must be installed in the NetShield server. If the server does not have a modem, send a Forward to a modem-equipped NetShield server.



Enter the server name as an Internet Protocol (IP) address, as a name your local domain name server can recognize, or in Universal Naming Convention (UNC) notation. Click OK to save your changes and return to the E-Mail Properties dialog box.



The Summary page lists all of the alert methods you've told NetShield to use to notify you when it finds a virus or other malicious code on your NetShield server. Click + next to each listed alert method to display the computers, printers, phone numbers, or e-mail addresses that will receive alert messages from NetShield. To remove an alert method, select it, then click Remove. To change the configuration options for a listed method, select it, then click Properties. Alert Manager will open the same property page you used to configure your options for that alert method.



Centralized Alerting is a powerful feature for alerting the appropriate personnel of workstation virus activity. Once Centralized Alerting is enabled and configured, workstations using Network Associates client antivirus software, such as VirusScan, report virus activity to NetShield servers. NetShield then notifies the appropriate personnel (through pagers, printers, e-mail, fax, etc.) listed in the [Alert Manager](#) Summary property page.

See also

{button ,JI(`alrtmgr.HLP`,`How_Centralized_Alerting_works`)} [How Centralized Alerting works](#)
{button ,JI(`alrtmgr.HLP`,`Configuring_Centralized_Alerting`)} [Configuring Centralized Alerting](#)
{button ,JI(`alrtmgr.HLP`,`Centralized_Alerting_file_format`)} [Centralized Alerting file format](#)



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

See also

{button ,JI(`alrtmgr.HLP`,`Configuring_Centralized_Alerting`)} [Configuring Centralized Alerting](#)

{button ,JI(`alrtmgr.HLP`,`Centralized_Alerting_file_format`)} [Centralized Alerting file format](#)



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

[CentralAlert]	Centralized Alerting identifier.
uFileVersion	Type: Integer Centralized Alerting version number.
uStatus	Reserved
szVirusName	Type: String The name of the virus.
szItemName	Type: String The infected file name and path.
szUserName	Type: String The user name.
szSoftware	Type: String The name of the Network Associates virus application installed on the reporting machine.
szSoftwareVersion	Type: String The version of the virus application.
szComputerName	Type: String The name of the machine reporting the event.
uYear	Type: Integer (0000-9999) The year of the event.
uMonth	Type: Integer (1-12) The month of the event.
uDay	Type: Integer (1-31) The day of the event.
uHour	Type: Integer (0-23) The hour of the event.
uMinute	Type: Integer (0-59) The minute of the event.

uSecond

Type: Integer (0-59)
The second of the event.



- 1 To configure Centralized Alerting, follow these steps:
- 2 Select Alerts from the Tools menu.
- 3 Select Enable Centralized Alerting (in most cases, Centralized Alerting is enabled by default).
- 4 Enter the location of the Alert Folder in the text box provided. You can click Browse to locate the Alert folder on the network. The default Alert folder is located in C:\Program\Mcafee\NetShield\Alert. All users must have create, write, and delete rights to the Alert Folder.
- 5 Click OK.
- 6 Configure the desktop machines which will report virus activity. For more information, refer to the documentation which accompanied VirusScan.



To enable and disable alerts, complete the following procedure.

- 1 Select Alerts from the Tools menu and click the Messages tab.
- 2 To enable an alert, select its checkbox.
- 3 To disable an alert, deselect its checkbox.
- 4 To save the changes and exit, click OK. To exit without saving changes, click Cancel.

See also

{button ,JI(`alrtmgr.HLP`,`Changing_the_priority_of_an_alert`)} [Changing the priority of an alert](#)

{button ,JI(`alrtmgr.HLP`,`Customizing_an_alert_message`)} [Customizing an alert message](#)

{button ,JI(`alrtmgr.HLP`,`Alert_Message_variables`)} [Alert message variables](#)



To change the priority level of an alert, follow these steps:

- 1 Select Alerts from the Tools menu and click the Messages tab.
- 2 Highlight an alert and click Edit.
- 3 Select a priority level.
- 4 Click OK.

See also

{button ,JI(`alrtmgr.HLP`,`Customizing_an_alert_message`)} [Customizing an alert message](#)

{button ,JI(`alrtmgr.HLP`,`Alert_Message_variables`)} [Alert message variables](#)

{button ,JI(`alrtmgr.HLP`,`Enabling_and_disabling_alerts`)} [Enabling and disabling alerts](#)



While an alert message can be customized, the reason for the alert does not change (e.g. when a task starts, the 'task has started' message is generated). Be careful not to modify the meaning of the alert message. Otherwise, notifications may become confusing or erroneous.

To customize an alert message, follow these steps:

- 1 Select Alerts from the Tools menu and click the Messages tab.
- 2 Highlight an alert and click Edit.
- 3 Enter a custom message in the text field.
- 4 Click OK.

See also

{button ,JI(`alrtmgr.HLP`,`Alert_Message_variables`)} [Alert message variables](#)

{button ,JI(`alrtmgr.HLP`,`Changing_the_priority_of_an_alert`)} [Changing the priority of an alert](#)

{button ,JI(`alrtmgr.HLP`,`Enabling_and_disabling_alerts`)} [Enabling and disabling alerts](#)



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
%COMPUTERNAME%	Name of the infected computer
%SOFTWARENAME%	Name of the software that detected the virus
%USERNAME%	Name of the local user
%SOFTWAREVERSION%	Version number of the software that detected the virus

