About Viruses

Computer viruses, most users know, can have a devastating impact on productivity. What many of those same users don't know is basic information that could help them protect themselves from infection—such as where viruses came from and how they operate.

In the beginning

The conceptual foundations for viruses have been around much longer than the virus threat itself. Although virus historians disagree on the specific whens and wheres, it is generally accepted that the ideas were born when computers were still huge and expensive—the domain of large corporations and the government, not the public. And while many of the viruses circulating today are malicious, destruction of data was not part of the original premise.

The idea was that if one could create a computer program that could make copies of itself, or self-replicate, it might also be possible for that program to evolve. If an error were to occur in the replication process, the resulting code (the bits of information that make up the program) would be mutant. Just as mutant genetic code is what disposes a biological virus to either be more or less able to survive and propagate, mutant digital code might dispose a computer virus to be more or less able to survive in the computer environment. Given enough time, the logical extension of the theory goes, a computer virus could evolve into something approaching artificial intelligence. Science fiction suddenly starts to look more like science and less like fiction.

What viruses really are

At its core, a virus is simply a program with one goal: self-replication. Part of achieving that goal is remaining undetected. If a virus is found by a user, it is likely to get deleted, which puts quite a damper on any self-replicating plans. Just like any other program, a virus has to be run to do its work. And since a user will not run a virus intentionally, the virus has to attach itself to a file that the user will run. That includes executable files and document files with embedded macros, as we will see in a couple of pages. For a virus to infect any other type of file—say, a plain text file—would be counter-productive: Remember, replication is its primary objective.

Computers with the sniffles?

Consider the similarities between computer and biological viruses. A computer virus infects a host program, just as a biological virus infects a host cell. It writes its own code in among the pieces of code that make up the host program. Then, in much the same way as a biological virus uses resources from its host organism to reproduce, a computer virus runs each time the infected host is run, and makes copies of itself. Those copies then infect other programs, and the cycle begins again.

Just as biological viruses have detrimental effects, so do their computer counterparts. The first computer viruses were simply experiments by research scientists to test the theory—to see if it could be done. They proved the theory, but also discovered that viruses had some unfortunate side effects. Viruses got in the way of some of the normal processes of the computer and caused erratic behavior. Many viruses are now specifically programmed to perform some function outside of self-replication. This function, called the payload, can be as innocuous as displaying a message on the computer's monitor or as harmful as destroying data on the system's hard disks. It is delivered when the trigger, an event such as a particular combination of keystrokes, a certain date or a pre-determined number of actions, occurs.

Who writes viruses?

The reason for this change in the behavior of viruses—from innocent experiment to malicious sneak attack—is a result of a change in the type of people who write them. Virus code is now developed by many people who are less interested in studying the possibility of artificial intelligence than in inflicting harm. Some do it out of spite, some because they aspire to be the underground "mad hacker" romanticized in much of pop culture as a freedom fighter of the digital age. The reasons people write virus code are probably as varied and strange as the reasons people perform other destructive acts.

Some virus writers actually choose to identify themselves, such as the Pakistani brothers who wrote the Brain virus. The brothers included the name, address, and telephone number of their software company in the viral code. When the payload was delivered, this information would be displayed for the user. Apparently, the brothers wrote the virus to show how widespread software pirating was. They put it on software leaving their office with the idea that wherever the virus spread, so had their software. Of course, what they overlooked was the fact that the virus spread by infecting programs other than the one it left their office in.

Other virus writers are disgruntled employees seeking revenge. Still others are schoolkids who write just to see if they can. The famous Stoned virus is said to have been written by such a youngster. Having written it, he feared the consequences of unleashing it, so he destroyed all copies of the virus except one, which he kept at his house. His younger brother and a couple of friends managed to lay their hands on it though, and infected some disks as a joke. But the infection spread quickly and soon was impossible to stop.

Whatever the motivation, the number of people capable of writing a virus is growing right alongside the computer industry. Those who stand to be affected by virus infection—anyone who uses a computer—should be alert and wary.

Only getting worse

In part, the fact that there are so many of us who need to be on the alert today is what makes virus proliferation possible. When the computer world was made up entirely of huge expensive machines, a virus did not have very far to go once it got started. But with the advent of the personal computer, viruses suddenly had a lot of places to go. The rapid growth of the Internet, the capability to attach files to e-mail messages, and the increasing degree to which the world depends on its computers all make conditions ever-better for the spread of computer viruses.

New developments

There are other reasons to be especially wary these days. Viruses get increasingly complex and advanced as computers on the whole do the same. Just in the last few years, sophisticated and dangerous new virus families have appeared, such as polymorphic viruses and macro viruses. Polymorphic viruses are especially tricky because they change each time they infect a new file. Where once anti-virus software could search for viruses by "signatures" (chunks of code unique to each virus), software must now be able to detect polymorphic viruses that change their signature each time they infect a file.

Macro viruses infect documents and document templates—new territory for viruses. Documents used to be safe from viral attack because until a few years ago, a document file didn't have any executable code in it. Now that software like Microsoft Word and Microsoft Excel has embedded macro capabilities, viruses can infect documents created by that software through the macro language.

All that just in the last few years. And viruses as a serious threat have only been around for about ten years. To imagine what is in store as the computer becomes more complicated and more a part of everyday life is frightening. Luckily, you have purchased the best protection against infection available today. With its outstanding support and worldwide anti-virus research teams, Network Associates makes sure your protection keeps up with the ever-changing computer world.

Features of VirusScan

- NCSA-certified scanner assures detection of 100% of viruses found "in the wild." See the NCSA website, www.NCSA.com, for certification status or click here  .
- VShield, VirusScan's on-access scanner, 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.
- Scan, VirusScan's on-demand scanner, provides for user-initiated detection of known boot, file, mutating, macro, stealth, and encrypted, viruses located within files, drives, and diskettes.
- VirusScan's new user interface offers flexible basic or advanced scanning options.
- Code Trace™, Code Poly™, and Code Matrix™ scanning employ proprietary Network Associates technologies for pinpoint virus identification accuracy.
- VirusScan can be configured for an automated response on virus detection, including notification, logging, deletion, isolation, or cleaning.
- The VirusScan Scan Window, Activity Log, and Virus List provide details of scan results, as well as information about detected viruses.
- Monthly updates of virus signatures are included with the purchase of a Network Associates subscription license to assure the best detection and removal rates. See Keeping VirusScan Updated.

Types of viruses

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

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

{button ,JI(`scan32.HLP',`Boot_virus')} Boot virus

{button ,JI(`scan32.HLP',`File_virus')} File virus

{button ,JI(`scan32.HLP',`Stealth_virus')} Stealth virus

{button ,JI(`scan32.HLP',`Multi_partite_virus')} Multi-partite virus

{button ,JI(`scan32.HLP',`Mutating_virus')} Mutating virus

{button ,JI(`scan32.HLP',`Encrypted_virus')} Encrypted virus

Boot Virus

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

File Virus

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

Stealth Virus

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

Multi-partite Virus

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

Mutating Virus

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

Encrypted Virus

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

Macro Virus

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.

Why Scan for Viruses?

In today's environment, safe computing practices are a necessity.

Computer viruses attack your computer through all computing environments you are in contact with through diskettes, networks, modems, and files you share with coworkers.

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.

Network Associates virus scanning solutions should top your list of safe computing practices. Scheduled periodic scans of your computer offer added assurance you are taking precautions against virus infection.

About Network Associates

Founded in 1986, 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 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 authorized agents in more than 50 countries worldwide.

Responding to a virus found in memory

If VirusScan discovers a virus in memory, complete the following procedure:

1 Turn off your computer.
2 Do not reboot using the reset button or Ctrl+Alt+Delete; if you do, some viruses might remain intact or drop their destructive payloads.
3 Place the Emergency Diskette into the floppy disk drive. See Making an Emergency Diskette.
4 Turn on your computer.
5 Follow the on-screen instructions and remove any viruses found.

If viruses were removed

If VirusScan successfully removes all the viruses, shut down your computer and remove the diskette.

To find and eliminate the source of infection, scan your diskettes immediately after installation.

If viruses were not removed

If VirusScan cannot remove a virus, the following message is displayed:

Virus could not be removed.

If the virus was found in a file and cannot be removed by VirusScan, you should delete the file and repeat the steps described above. If the virus was found in the Master Boot Record, refer to documents on the Network Associates website related to manually removing viruses. For more information, see Contacting Network Associates.

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

Understanding false alarms

A false alarm is a report of a virus in a file or in memory when a virus does not actually exist. False alarms are more likely if you are using more than one brand of virus protection software, because some anti-virus programs store their virus signature strings unprotected in memory.

Always assume that any virus found by VirusScan is real and dangerous, and take necessary steps to remove it from your system. If, however, you have reason to believe that VirusScan is generating false alarms (for example, it has detected a virus in only one file that you have been using safely for years), refer to the list of potential sources below:

- If more than one anti-virus program is running, VirusScan may report a false alarm. Set up your computer so that only one anti-virus program is running at a time. Remark out lines in the AUTOEXEC.BAT file that refer to other anti-virus programs. Turn off your computer, wait a few seconds, and turn it on again to make sure that all code from other anti-virus programs is cleared from memory.
- Some BIOS chips include an anti-virus feature that could be the source of false alarms. Refer to your computer's reference manual for details.
- If you set up validation/recovery codes, subsequent scans can detect changes in validated files. This can trigger false alarms if the executable files are self-modifying or self-checking. When using validation codes, specify an exceptions list to exclude such files from checking.
- Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. VirusScan may detect these modifications as a possible infection, even though no virus may be present. Check your computer's reference manual to determine if your PC has self-modifying boot code. To solve this problem, save validation/recovery information to the executable files themselves; this method does not save information about the boot sector or Master Boot Record.
- VirusScan may report viruses in the boot sector or Master Boot Record of certain copy-protected diskettes.

Maintaining a secure environment

VirusScan is an effective tool for preventing, detecting, and recovering from virus infection. It is most effective, however, when used in conjunction with a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness.

Keeping VirusScan Updated

To offer the best virus protection possible, Network Associates continually updates the files VirusScan uses to detect viruses. After a certain time period, VirusScan will notify you to update the virus definition database. For maximum protection, it is important to update these files on a regular basis.

What is a data file?

The files CLEAN.DAT, NAMES.DAT, MCALYZE.DAT, and SCAN.DAT all provide virus information to the VirusScan software and make up the data files referred to in this section.

Why would I need a new data file?

New viruses are discovered at a rate of more than 200 a month. Often, these viruses are not detected using older data files. The data files that came with your copy of VirusScan may not detect a virus that was discovered after you bought the product.

Network Associates virus researchers are working constantly to update the data files with more and newer virus definitions. The new data files are released approximately every four to six weeks.

To update VirusScan, select from the following:

{button ,JI(`>(w95sec)',`Updating_VirusScan_using_Electronic_Update')} Electronic Update

{button ,JI(`>(w95sec)',`Updating_VirusScan_manually')} Manual Update

Note

- Network Associates cannot guarantee backward compatibility of the virus signature files with a previous version's software. By subscribing to a maintenance plan and upgrading your VirusScan software, you ensure complete virus protection for the duration of the plan.

Updating VirusScan using Electronic Update

VirusScan will inform you when your data files are dangerously out of date or your evaluation copy of VirusScan is expired. With this feature, you can easily update your data files or register your software electronically. When prompted, click Update or Purchase and follow the on-screen instructions.

To start Electronic Update from the VirusScan main window, select Update VirusScan from the File Menu and follow the on-screen instructions.

To update VirusScan manually

1 Download the data file (for example, DAT-3006.ZIP) from one of the Network Associates electronic services. On most services, it is located in the anti-virus area.
2 Copy the file to a new folder.
3 The file is in a compressed format. Decompress the file using any PKUNZIP-compatible decompression software. If you don't have the decompression software, you can download PKUNZIP (shareware) from Network Associates electronic services.
4 Copy the new data files to the VirusScan folder. The default VirusScan folder is C:\Program Files\McAfee\VirusScan.

Tip

- To visit the Network Associates website, click here  .

Note

- Please note that your ability to access these updates is legally restricted by the maintenance terms outlined in the README.1ST file accompanying the software and detailed in the software license agreement.

Making the Emergency Disk

The Emergency Disk is a very important part of proper virus prevention. Should your system become infected, the Emergency Disk will enable you to start your computer from a clean environment.

To make an Emergency Disk, complete the following procedure:

1 Format a 3.5" 1.44MB floppy disk using DOS or Windows Explorer with the system files option.

2 Click Start, point to Programs, point to McAfee VirusScan, and click Create Emergency Disk, or click here  . The Emergency Disk Creation Utility Welcome screen is displayed.

3 Click **OK**. The Utility begins creating the Emergency Disk.

4 When the Utility is finished, remove the disk, write-protect it, label it "VirusScan Emergency Disk", and store it in a safe place.

Note

- If you use a disk compression utility or a password encryption utility, be sure to copy the drivers required to access your drives onto the Emergency Disk. For more information, see the documentation which accompanied those utilities.

Insert a floppy disk and try again

To format a diskette using DOS

Click here  .or enter the following command from the DOS prompt:

```
format a: /s
```

To format a diskette using Windows Explorer

1 Insert a floppy disk into the A:\ drive.

2 Open Windows Explorer or click here  .

3 Right-click the 3½" Floppy Icon and select Format from the shortcut menu. The Format dialog box is displayed.

4 Select Full from the Format Type options.

5 Select Copy System Files from the Other options.

6 Click Start. Windows Explorer begins formatting the diskettes.

Write-protecting diskettes

Floppy diskettes are convenient, portable devices for storage and retrieval of computer data. Diskettes are used to save files (write) and recover files (read). They are also the most common vehicle viruses use to invade your computer's system.

One way to help prevent infection via floppy diskette is to write-protect diskettes you are using for read-only data. If your system becomes infected with a virus, the write-protection feature keeps your diskettes from becoming infected, preventing reinfection after your system is cleaned.

To write-protect a 3.5" floppy disk:

1 Position the diskette face down with the metal slide facing you.
2 Examine the small rectangular hole on the upper left side. There should be a square, plastic tab that you can slide up and down across the hole.
3 To write-protect the diskette, slide the plastic tab upward toward the edge of the diskette so that the hole is open.

Notes

- Any diskettes that are not write-protected should be scanned and cleaned before you write-protect them.
- If there is no tab and the hole is open, the diskette is write-protected.

Contacting Network Associates

Select from the following:

{button ,JI(`scan32.HLP',`Customer_Service')} Customer Service

{button ,JI(`scan32.HLP',`Technical_Support')} Technical Support

{button ,JI(`scan32.HLP',`Network_Associates_Training')} Training

Customer Service

To order products or obtain product information, we invite you to contact our Customer Care department at (972) 278-6100 for retail customers or (408) 988-3832 for corporate customers. Or, contact us at the following address:

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

Technical Support

Network Associates is famous for its dedication to customer satisfaction and has continued this tradition by making the Network Associates website a valuable resource for answers to technical support issues. Network Associates encourages you to make this your first stop for answers to frequently asked questions, for updates to Network Associates software, and for access to Network Associates news and virus information

World Wide Web	http://www.nai.com

Click here  to access the Network Associates website.

If you do not find what you need or do not have access to the Web, try one of the Network Associates automated services.

Automated Voice and Fax Response System	(408) 988-3034
Internet	support@nai.com
Network Associates BBS	(408) 988-4004 1200 bps to 28,800 bps 8 bits, no parity, 1 stop bit 24 hours, 365 days a year
CompuServe	GO MCAFEE
America Online	Keyword MCAFEE

If the automated services did not solve your problem, you may contact Network Associates Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

Retail Customer Phone	(972) 278-6100
Corporate Customer Phone	(408) 988-3832
Fax	(408) 970-9727

To speed the process of helping you use our products, please note the following before you call:

- Product name and version
- Computer brand, model, and any additional hardware
- Operating system type and version
- Network type and version
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem, if applicable

Network Associates Training

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

VirusScan for DOS Error Levels

When you run VirusScan in the DOS environment (using SCAN.EXE), a DOS error level is set. You can use the ERRORLEVEL in batch files to take different actions based on the results of the scan. For more information, see your DOS operating system documentation.

VirusScan can return the following error levels:

ERROR LEVEL	Description
0	No errors occurred; no viruses were found.
1	Error occurred while accessing a file (reading or writing).
2	A VirusScan data file is corrupted.
3	An error occurred while accessing a disk (reading or writing).
4	An error occurred while accessing the file created with the /AF option; the file has been damaged.
5	Insufficient memory to load program or complete operation.
6	An internal program error has occurred (out of memory error).
7	An error occurred in accessing an international message file (MCAFEE.MSG).
8	A file required to run VirusScan, such as SCAN.DAT, is missing.
9	Incompatible or unrecognized option(s) or option argument(s) specified in the command-line.
10	A virus was found in memory.
11	An internal program error occurred.
12	An error occurred while attempting to remove a virus, such as no CLEAN.DAT file found, or VirusScan was unable to remove the virus.
13	One or more viruses were found in the Master Boot Record, boot sector, or files.
14	The SCAN.DAT file is out of date; upgrade VirusScan data files.
15	VirusScan self-check failed; it may be infected or damaged.
16	An error occurred while accessing a specified drive or file.
17	No drive, folder, or file was specified; nothing to scan.
18	A validated file has been modified (/CF or /CV options).
19-99	Reserved.
100+	Operating system error; VirusScan adds 100 to the original number.
102	CTRL+C or CTRL+BREAK was used to interrupt the Scan. (You can disable CTRL+C or CTRL+BREAK with the /NOBREAK command-line option.)

Safe Computing Practices

Safe computing practices include:

Virus protection
Regular backups
Meaningful password protection
Training and awareness

Move Infected Files

When this option is selected, infected files are automatically moved to the specified folder. To select a quarantine location, enter the path to a folder or click **Browse** to locate one.

Clean Infected Files

When this option is selected, viruses are automatically removed from files. If a virus could not be removed, run VirusScan with the delete option and restore the infected file from backups.

Delete Infected Files

When this option is selected, infected files are automatically deleted. After VirusScan deletes the infected files, you can restore them from backup.

If you select this option, make sure to enable report logging. This will ensure you have a record of which files were deleted, so you can restore them from backups.

Continue Scanning

When this option is selected, scanning continues and no action is taken. When the scan is complete, you can manually respond to each infected file in the VirusScan Main Window.

Note

- This option is not recommended for unattended machines.

Prompt for Action

When this option is selected, you are prompted for action for each infected file. To make an action available or not available on virus detection, select or deselect its checkbox.

Tip

- To prevent access to specific actions, such as Continue Scanning (without taking any action), deselect their checkboxes and enable Password Protection.

Virus Name

Lists the name of the virus

Infects

Indicates the types of files infected by this virus. This may include:

Executables (.EXE)
COM files (.COM)
Word files (.DO?)
Excel files (.XL?)

Virus Size

Indicates the size of the virus in bytes.

Memory Resident

Indicates whether the virus resides in memory.

Encrypted

Indicates whether this is an encrypted virus.

Polymorphic

Indicates whether this is a polymorphic virus. Polymorphic viruses modify their code to avoid detection.

Repairable

Indicates whether files infected by this virus are repairable.

Macro Virus

Indicates whether this is a macro virus. Macro viruses infect Microsoft Word and Excel files.

Program Files

Program files are file types which are most susceptible to virus infections. These include .COM, .EXE, .DO?, .XL?. To change which file types are scanned for viruses, complete the following procedure:

1 Click **Extensions**. The Program File Extensions dialog box is displayed.
2 To add a file extension to scan, click Add. Enter a new file extension and click **OK**. Repeat this step until all desired file extensions have been entered.
3 To delete an extension, select it and click Delete.
4 To return to the default extensions, click Default.
5 To exit without saving changes to the program files list, click cancel. To save the changes and exit, click **OK**.

Compressed Files

When enabled, VirusScan scans PKZIP, PKLITE, WInZip, LZH, and LZEXE compressed files.

Compressed Files

When enabled, VShield scans PKLITE and LZEXE compressed files.

To open Windows Explorer

Click Start, point to Programs, and click Windows Explorer.

To open My Computer

Locate and double-click the My Computer icon in the upper left-hand corner of the desktop.

Centralized Alerting

Centralized Alerting is a Network Associates enterprise-wide virus notification solution. Once configured, workstations running VirusScan send virus notifications to servers running NetShield. This helps administrators locate the source of the virus infections and prevent them from spreading.

To configure Centralized Alerting, do the following:

1 Ask a system administrator for the name of a server running NetShield and its Centralized Alerting Folder.

2 Make sure you have rights to write to this folder.

3 Configure VShield and VirusScan tasks to send network messages to this folder.

Notes

- To configure VShield and VirusScan tasks to send Centralized Alerting messages to a server, select Send Network Alert on the Action page and click **Browse** to locate the server's Centralized Alerting folder.
- A file named CENTALRT.TXT must be located in the server's Centralized Alerting folder.

Virus Information Library

The Virus Information Library contains detailed virus information. This information includes the virus name, its characteristics, its method of infection, how to tell if you are infected, and how it can be removed.

- To see the current version of the Virus Information Library, click here  .
- To find the Virus Information Library on the Network Associates website, go to this address: http://www.nai.com/vinfo.

Notes

- To see the Virus Information Library, you must have an active connection to the Internet and you must have a copy of Netscape Navigator or Microsoft Internet Explorer. If you do not have one of these browsers, but you do have access to the World Wide Web, use your browser software to connect to the Network Associates website listed above.

Testing Your Installation

The Eicar Standard AntiVirus Test File is a world-wide combined effort by anti-virus vendors to set one standard for customers to verify their anti-virus installations. To test your installation, copy the following line into its own file and name it EICAR.COM:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Upon completion, you will have a 69- or 70-byte file.

When this file is scanned, VirusScan will report finding the EICAR-STANDARD-AV-TEST-FILE virus.

THIS FILE IS NOT A VIRUS! Delete the file when installation testing is completed so unsuspecting users are not unnecessarily alarmed.

Note

- Because the Eicar Standard AntiVirus Test File is not a true virus infection, you will not be able to clean or repair the infected file.

VSH File Format

The VSH file is a configuration text file, formatted similarly to the Windows INI file, which outlines VShield's settings. Each variable in the file has a name followed by the equal (=) sign and a value. The values define which settings have been selected for VShield configuration. The variables are arranged in five groups: DetectionOptions, ActionOptions, ReportOptions, General, and ExcludedItems. To edit the VSH file, right-click on the filename and select Edit.

In Boolean variables, possible values are 0 and 1. The 0 value instructs VShield to disable the setting, while 1 indicates that the setting is enabled.

General

Variable	Description
bCanBeDisabled	Type: Boolean (1/0) Defines if VShield can be disabled Default value: 1
bShowTaskbarIcon	Type: Boolean (1/0) Defines whether VShield taskbar icon is displayed Default value: 1

DetectionOptions

Variable	Description
bScanOnExecute	Type: Boolean (1/0) Instructs VShield to scan when files are run Default value: 1
bScanOnOpen	Type: Boolean (1/0) Instructs VShield to scan when files are opened Default value: 1
bScanOnCreate	Type: Boolean (1/0) Instructs VShield to when files are created Default value: 1
bScanOnRename	Type: Boolean (1/0) Instructs VShield to when files are renamed Default value: 1
bScanOnShutdown	Type: Boolean (1/0) Instructs VShield to scan the boot record of drive A: when system is shut down Default value: 1
bScanOnBootAccess	Type: Boolean (1/0) Instructs VShield to scan the boot record of a disk drive the first time it is accessed Default value: 1
bScanAllFiles	Type: Boolean (1/0) Instructs program to scan inside all files Default value: 0
bScanCompressed	Type: Boolean (1/0) Instructs program to scan compressed files. Default value: 0

szProgramExtensions	Type: String Defines extensions to be scanned Default value: EXE COM DO? XL?
szDefaultProgramExtensions -	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: EXE COM DO? XL?

AlertOptions

Variable	**Description**
bNetworkAlert	Type: Boolean (1/0) Enables Centralized Alerting Default value: 0
szNetworkAlertPath	Type: String Specifies a server's Centralized Alerting folder. Default value: none

ActionOptions

Variable	Description
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed in the Prompt for Action dialog box upon virus detection Default value: 0
uVshieldAction	Type: Integer (1-5) Instructs VShield to take the action specified when a virus is detected Possible values: 1 - Prompt for action 2 - Move infected files to a folder 3 - Clean infected files automatically (Deny access if files can't be cleaned) 4 - Delete infected files automatically 5 - Deny access to infected files Default value: 1
bButtonClean	Type: Boolean (1/0) Instructs VShield to give user option of cleaning file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonDelete	Type: Boolean (1/0) Instructs VShield to give user option of deleting file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonExclude	Type: Boolean (1/0) Instructs VShield to give user option of excluding file if Prompt for Action is selected and a virus is detected Default value: 1

bButtonContinue	Type: Boolean (1/0) Instructs VShield to give user option of continuing the intercepted event if Prompt for Action is selected and a virus is detected Default value: 1
bButtonStop	Type: Boolean (1/0) Instructs VShield to give user option of denying access to the infected file if Prompt for Action is selected and a virus is detected Default value: 1
szMoveToFolder	Type: String Defines folder to which infected files should be moved Default value: \Infected
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection if action is set to Prompt for Action Default value: Possible Virus Found

ReportOptions

Variable	**Description**
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 0
bLimitSize	Type: Boolean (1/0) Defines if size of the log file should be limited Default value: 1
uMaxKilobytes	Type: Integer (10-999) Defines maximum size of the log file in kilobytes Default value: 100
bLogDetection	Type: Boolean (1/0) Defines if scanning results should be logged Default value: 1
bLogClean	Type: Boolean (1/0) Defines if cleaning 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 on shutdown Default value: 1
bLogSummary	Type: Boolean (1/0) Defines if session summary should

	be logged on shutdown 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
szLogFileName	Type: String Defines log file name Default value: C:\Program Files\McAfee\VirusScan\VSHLOG.TXT

SecurityOptions

Variable	**Description**
szPasswordProtect	Type: Boolean (1/0) Defines if password protection is enabled. Default value: 0

ExclusionOptions

Variable	**Description**
szExclusionsFileName	Type: String Default value: VSHLOG.TXT

AVCONFILE

Variable	**Description**
AVCONFILE	Type: String Specifies the path to AVCONSOLE Default: C:\Program Files\McAfee\VirusScan\avconsole.ini
SECTION	Type:String Specifies the reporting location within AVCONSOL.INI Default: Item_0

ExcludedItems

Variable	**Description**
NumExcludedItems	Type: Integer (0-n) Defines the number of items excluded from on-access scanning Default value: 1
ExcludedItem_x, where x is a zero-based index	Type: String Instructs VShield to exclude the item from on-access scanning Default value: \Recycled|*.*|1|1 * * The string is separated into fields using the pipe (|) character:

Field 1 - Folder portion of item to exclude. Leave blank for a single file anywhere on the system.

Field 2 - File portion of the item to exclude. Leave blank if a folder is excluded without a filename.

Field 3 - Integer (1-3)

Possible values:

1 - Exclude from file-access scanning

2 - Exclude from boot-record scanning

3 - Exclude from both boot-record and file-access scanning

Field 4 - Boolean (1/0)

Possible values:

1 - Instructs VShield to exclude subfolders of the excluded item

0 - Instructs VShield to not exclude subfolders

VSC File Format

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 have been selected for VirusScan configuration. The variables are arranged in three groups: ScanOptions, AlertOptions, and ActivityLogOptions. To edit the VSC file, right-click on the filename and select Edit.

Note

- In Boolean variables, possible values are 0 and 1. The 0 value instructs VirusScan to disable the setting, while 1 indicates that the setting is enabled.

ScanOptions

Variable	Description
bAutoStart	Type: Boolean (1/0) Instructs VirusScan to start scanning immediately as it is launched Default value: 0
bAutoExit	Type: Boolean (1/0) Instructs VirusScan to exit upon scan completion if no viruses are found Default value: 0
bAlwaysExit	Type: Boolean (1/0) Instructs VirusScan to always exit upon scan completion Default value: 0
bSkipMemoryScan	Type: Boolean (1/0) Instructs VirusScan to skip memory scan Default value: 0
bSkipBootScan	Type: Boolean (1/0) Instructs VirusScan to skip boot sector scan Default value: 0
bSkipSplash	Type: Boolean (1/0) Instructs VirusScan to not display the initial splash screen when the application is launched Default value: 0
nPriority	Type: Integer (0-5) Specifies the scanning threads priority. Possible values: 0 - Normal (default) thread priority 1 - Lowest thread priority 2 - Below normal thread priority 3 - Normal thread priority 4 - Above normal thread priority 5 - Highest thread priority Default value: 0
nChecksum	Reserved
bConfigurableGuiMode	Type: Boolean (1/0) Instructs VirusScan to use the Advanced user interface Default value: 0
szTaskName	Reserved

DetectionOptions

Variable	Description

bScanAllFiles	Type: Boolean (1/0) Instructs VirusScan to scan inside all files Default value: 0
bScanCompressed	Type: Boolean (1/0) Instructs VirusScan to scan compressed files Default value: 1
szProgramExtensions	Type: String Defines extensions to be scanned Default value: COM DO? EXE XL?
szDefaultProgramExtensions	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: COM DO? EXE XL?

AlertOptions

Variable	Description
bNetworkAlert	Type: Boolean (1/0) Enables Centralized Alerting Default value: 0
bSoundAlert	Type: Boolean (1/0) Instructs VirusScan to sound an alert when a virus is detected Default value: 1
szNetworkAlertPath	Type: String Specifies a server's Centralized Alerting folder. Default value: none

ActionOptions

Variable	Description
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed upon virus detection Default value: 0
uScanAction	Type: Integer (1-5) Instructs VirusScan to take the action specified when a virus is detected Possible values: 0 - Prompt for action 1 - Move infected files to a folder 2 - Clean infected files automatically 3 - Delete infected files automatically 4 - Continue scanning Default value: 0
bButtonClean	Type: Boolean (1/0) Instructs VirusScan to give user option of cleaning the file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonDelete	Type: Boolean (1/0) Instructs VirusScan to give user option

	of deleting the file if Prompt for Action is selected and a virus is detected
	Default value: 1
bButtonExclude	Type: Boolean (1/0)
	Instructs VirusScan to give user option of excluding the file if Prompt for Action is selected and a virus is detected
	Default value: 0
bButtonMove	Type: Boolean (1/0)
	Instructs VirusScan to give user option of moving the infected file if Prompt for Action is selected and a virus is detected
	Default value: 1
bButtonContinue	Type: Boolean (1/0)
	Instructs VirusScan to give user option of continuing the scan if Prompt for Action is selected and a virus is detected
	Default value: 1
bButtonStop	Type: Boolean (1/0)
	Instructs VirusScan to give user option of denying access to the infected file if Prompt for Action is selected and a virus is detected
	Default value: 1
szMoveToFolder	Type: String
	Defines folder to which infected files should be moved
	Default value: \Infected
szCustomMessage	Type: String
	Defines custom message to be displayed upon virus detection
	Default value: Possible Virus Found

ReportOptions

Variable	**Description**
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 log file in kilobytes
	Default value: 100
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 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 on shutdown
	Default value: 1
bLogSummary	Type: Boolean (1/0)
	Defines if session summary should be logged on shutdown
	Default value: 1
bLogDateTime	Type: Boolean (1/0)
	Defines if date and time of an event should be logged
	Default value: 1
bLogUserName	Type: Boolean (1/0)
	Defines if user name should be logged
	Default value: 1
szLogFileName	Type: String
	Defines log file name
	Default value: VSCLOG.TXT

ScanItems

Variable	**Description**
NumScanItems	Type: Integer (0-n)
	Defines the number of items to scan
	Default value: 1
szScanItem_x	Type: String
	Default value: C:\
	Instructs Vshield to scan the item
	* The string is separated into fields using the pipe (|) character:
	Field 1 - Folder portion of item to scan. Leave blank for a single file anywhere on the system.
	Field 2 - File portion of the item to scan. Leave blank if a folder is scanned without a filename.
	Field 3 - Integer (1-3)
	Possible values:
	1 - Scans file
	2 - Scans boot-record
	3 - Scans from both boot-record and file
	Field 4 - Boolean (1/0)
	Possible values:
	1 - Instructs VShield to scan subfolders of the item
	0 - Instructs VShield to not scan subfolders of the item

SecurityOptions

Variable	**Description**

szPasswordProtect	Type: Boolean (1/0) Defines if password protection is enabled. Default value: 0
szPasswordCRC	Reserved. Do not modify.
bInheritSecurity	Type: Boolean (1/0) Defines if the Inherit Security feature is enabled. When enabled, copies of the task remain password protected Default value: 0

ExcludedItems

Variable	**Description**
NumExcludeItems	Type: Integer (0-n) Defines the number of items excluded from on-access scanning Default value: 1
ExcludedItem_x, where x is a zero-based index	Type: String Instructs Vshield to exclude the item from on-access scanning Default value: \Recycled|*.*|1|1 * * The string is separated into fields using the pipe (|) character: Field 1 - Folder portion of item to exclude. Leave blank for a single file anywhere on the system. Field 2 - File portion of the item to exclude. Leave blank if a folder is excluded without a filename. Field 3 - Integer (1-3) Possible values: 1 - Exclude from file-access scanning 2 - Exclude from boot-record scanning 3 - Exclude from both boot-record and file-access scanning Field 4 - Boolean (1/0) Possible values: 1 - Instructs VShield to exclude subfolders of the excluded item 0 - Instructs VShield to not exclude subfolders

Centralized Alerting ALR File Format

The ALR file is the Centralized Alerting text that contains 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.

VirusScan for DOS Command-line Options

The following table lists all of the options you can use when you're running the DOS command-line program, SCAN.EXE. To run SCAN.EXE, first use the cd command to change directories to the folder where VirusScan is installed. Then, type scan /? to display a list of options and descriptions of how they can be used.

Notes

- When specifying a filename as part of a command-line option, you must include the full path to the file if it is not located in the folder where VirusScan is installed.
- These options are only available for SCAN.EXE and are can only be used at the DOS command-line prompt.

Tip

- To scan all system drives (including compressed drives and locally mapped CD-ROM and PCMCIA drives—but not diskettes) for known viruses, enter the following command:

  scan /adl

Command-line Option	Description
`/?` or `/HELP`	Does not scan. Instead, displays a list of VirusScan command-line options with a brief description of each. Use either of these options alone on the command-line (with no other options).
/ADL	Scans all local drives (including compressed, CD-ROM, and PCMCIA drives, but not diskettes), in addition to those specified on the command-line. To scan both local and network drives, use /ADL and /ADN together in the same command-line.
/ADN	Scans all network drives for viruses, in addition to those specified on the command-line. To scan both the local drives and network drives, use /ADL and /ADN together in the same command-line.
/AF filename	Stores validation/recovery codes in *filename.* Helps you detect new or unknown viruses. /AF logs validation and recovery data for executable files, the boot sector, and Master Boot Record on a hard disk or diskette in a file you specify. The log file is about 89 bytes per file validated. You must specify a *filename*, which can include the full path. If the target path is a network drive, you must have rights to create and delete files on that drive. If *filename* exists, VirusScan updates it. /AF adds about 300% more time to scanning. */AF performs the same function as /AV, but stores its data in a separate file rather than changing the executable files themselves.* The /AF option does not store any information about the Master Boot Record or boot sector of the drive being scanned.
/ALERTPATH folder	Specifies the Centralized Alerting network folder monitored by NetShield. See Centralized Alerting.
/ALL	Overrides the default settings by scanning all files. This option substantially increases the scanning time required. Use it if you have found a virus or suspect one.

	The list of extensions for standard executables has changed from previous releases of VirusScan.
/APPEND	Used in conjunction with /REPORT, appends the report message text to the specified report file, if it exists. Otherwise, the /REPORT option overwrites the specified report file, if it exists.
/AV	To help you detect and recover from new or unknown viruses, /AV adds recovery and validation data to each standard executable file (.EXE, .COM, .SYS, .BIN, .OVL, and .DLL), increasing the size of each file by 98 bytes. To update files on a shared network drive, you must have update access rights. To exclude self-modifying or self-checking files, and damaged files that might cause false alarms, use the /EXCLUDE option. Using any of the /AV, /CV, or /RV options together in the same command-line returns an error. *The /AV option does not store any information about the Master Boot Record or boot sector of the drive being scanned.*
/BOOT	Scans only the boot sector and Master Boot Record on the specified drive.
/CF filename	Helps you detect new or unknown viruses. Checks validation data stored by the /AF option in *filename*. If a file or system area has changed, VirusScan reports that a viral infection may have occurred. The /CF option adds about 250% more time to scanning. Using any of the /AF, /CF, or /RF options together in a command-line returns an error. *Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. If you use /CF, VirusScan continuously reports that the boot sector has been modified even though no virus may be present. Check your computer's reference manual to determine whether your PC has self-modifying boot code.*
/CLEANDOC	Cleans viruses from infected Microsoft Word files only.
/CLEANDOCALL	Removes all macros from infected Microsoft Word files.
/CONTACTFILE filename	Identifies a file containing a message string to display when a virus is found. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation. Any character is valid except a backslash (\). Messages that begin with a slash (/)or a hyphen (-) should be placed in quotation marks.
/CV	Helps you detect new or unknown viruses. Checks validation data added by the /AV option. If a file is modified, VirusScan reports that a viral infection may have occurred. The /CV option adds about 50% more time to scanning. Using any of the /AV, /CV, or /RV options together in the same command-line returns an error.

	The /CV option does not check the boot sector for changes.
/DEL	Deletes any infected files. Once deleted, restore the infected files from backup.
/EXCLUDE filename	Excludes any files listed in *filename* from the scan. This option allows you to exclude files from /AF and /AV validation and /CF and /CV checking. Self-modifying or self-checking files can cause a false alarm during a scan.
/FAST	Speeds up the scan. Reduces scanning time by about 15%. Using the /FAST option, VirusScan examines a smaller portion of each file for viruses. Using /FAST might miss some infections found in a more comprehensive (but slower) scan. Do not use this option if you have found a virus or suspect one.
/FORCE	Uses the generic master boot record when cleaning partition table viruses.
/FREQUENCY hours	The number of hours that must occur between subsequent successful scans (Example: `/FREQUENCY 1`). In environments where the risk of viral infection is very low, use this option to prevent unnecessary or too-frequent scans. The lower the number of *hours* specified, the greater the scan frequency and the greater your protection against infection.
/LOAD filename	Performs a scan using the information saved in *filename*. You can store all custom settings in a separate configuration file (an ASCII text file), then use /LOAD to load those settings from that file.
/LOCK	Halts the system to stop further infection if VirusScan finds a virus. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. If you use /LOCK, we recommend you use it with /CONTACTFILE to tell users what to do or whom to contact if a virus is found and the system locks up.
/LOG	Stores the time and date VirusScan is being run by updating or creating a file called SCAN.LOG in the root of the current drive.
/MANY	Scans multiple diskettes consecutively in a single drive. VirusScan prompts you for each diskette. Once you have established a virus-free system, use this option to check multiple diskettes quickly. The VirusScan program should reside on a disk that will not be removed during the scan. For example, if you are scanning disks in the computer's A: drive, and you are running the program from a disk in the A: drive, the program will become unavailable as soon as you remove the diskette to put another in. The following command causes an error during execution: a:\scan a: /many
/MAXFILESIZE xxx.x	Specifies the maximum size of files scanned for viruses.
/MEMEXCL	Exclude memory area from scanning. (The

	default is A000-FFFF, 0000=Scan all.)
	This command-line option has been added to prevent VirusScan from checking areas in upper memory which might contain memory-mapped hardware and might cause false alarms.
/MOVE directory	Moves all infected files found during a scan to the specified directory. To preserve drive and directory structure, this option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files.
/NOBEEP	Disables the tone that sounds whenever VirusScan finds a virus.
/NOBREAK	Disables ctrl-c and ctrl-break during scans.
	Users will not be able to halt scans in progress using ctrl-c or ctrl-break. Use this option in conjunction with /LOG to create a meaningful audit trail of regularly scheduled scans.
/NOCOMP	Skips checking of compressed executables created with the LZEXE or PKLITE file-compression programs.
	Reduces scanning time when a full scan is not needed. Otherwise, by default, VirusScan checks inside executable, or self-decompressing, files that have been created using the LZEXE or PKLITE file-compression programs. VirusScan decompresses each file in memory and checks for virus signatures, which takes time but results in a more thorough scan. If you use /NOCOMP, VirusScan does not check inside compressed files for viruses, although it can check for modifications to those files if they have been validated using validation/recovery codes.
/NODDA	No direct disk access.
	Prevents VirusScan from accessing the boot record. This feature has been added to allow VirusScan to run under Windows NT.
	You might need to use this option on some device-driven drives.
/NODOC	Skips scanning of Microsoft Word files.
/NOEMS	Prevents VirusScan from using expanded memory (LIM EMS 3.2), ensuring that EMS is available to other programs.
/NOEXPIRE	Disables the ‘‘expiration date’’ message if the VirusScan data files are out of date.
/NOMEM	Reduces scan time by omitting all memory checks for viruses. Use /NOMEM only when you are absolutely certain that your computer is virus-free.
	VirusScan can check system memory for all critical known computer viruses that can inhabit memory. In addition to main memory from 0kb to 640kb, VirusScan checks system memory from 640kb to 1088kb that can be used by computer viruses on 286 and later systems. Memory above 1088kb is not addressed directly by the processor and is not presently susceptible to viruses.
/PAUSE	Enables screen pause.
	If you specify /PAUSE, the ‘‘Press any key to continue’’ prompt appears when VirusScan fills up a screen with messages (for example, when you’re using the /SHOWLOG or /VIRLIST options). Otherwise, by default,

	VirusScan fills and scrolls a screen continuously without stopping, which allows VirusScan to run on PCs with many drives or that have severe infections without requiring you to attend. We recommend that you omit /PAUSE when keeping a record of VirusScan's messages using the report options (/REPORT, /RPTCOR, /RPTMOD, and /RPTERR).
/PLAD	Preserve last access dates (on proprietary drives only). Prevents changing the last access date attribute for files stored on a network drive in a proprietary network. Normally, proprietary network drives update the last access date when VirusScan opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use /PLAD to ensure that the last access date does not change as the result of scanning.
/REPORT filename	Creates a report of infected files and system errors. Saves the output of VirusScan to *filename* in ASCII text file format. If *filename* exists, /REPORT erases and replaces it (or, if you use /APPEND, adds the report information to the end of the existing file). You can include the destination drive and directory (such as D:\VSREPRT\ALL.TXT), but if the destination is a network drive, you must have rights to create and delete files on that drive. You can also use /RPTALL, /RPTCOR, /RPTMOD, and /RPTERR to add scanned files, corrupted files, modified files, and system errors to the report.
/RF filename	Removes recovery and validation data from *filename* created by the /AF option. If *filename* resides on a shared network drive, you must be able to delete files on that drive. Using any of the /AF, /CF, or /RF options together in the same command-line returns an error.
/RPTALL	Adds list of files scanned to the report file (used with /REPORT).
/RPTCOR	When used in conjunction with /REPORT, adds the names of corrupted files to the report file. A corrupted file may be a file that has been damaged by a virus. You can use /RPTCOR with /RPTMOD and /RPTERR on the same command-line. *There may be false readings in some files that require an overlay or another executable to run properly (that is, a file that is not executable on its own).*
/RPTERR	Adds a list of system errors to the report file. This option is used in conjunction with /REPORT. System errors include problems reading or writing to a diskette or hard disk, file system or network problems, problems creating reports, and other system-related problems. You can use /RPTERR with /RPTCOR and /RPTMOD on the same command-line.

/RPTMOD	Adds list of modified files to the report file. This option is used in conjunction with /REPORT. VirusScan identifies modified files when the validation/recovery codes do not match (using the /CF or /CV options). You can use /RPTMOD with /RPTCOR and /RPTERR on the same command-line.
/RV	Removes validation and recovery data from files validated with the /AV option. To update files on a shared network drive, you must have access rights to update them. Using any of the /AV, /CV, or /RV options together in the same command-line returns an error.
/SHOWLOG	Displays the contents of SCAN.LOG. SCAN.LOG stores the time and date VirusScan is being run by updating or creating a file called SCAN.LOG in the current directory and the date and time of previous scans that have been recorded in the SCAN.LOG file using the /LOG switch. The SCAN.LOG file contains text and some special formatting. To pause when the screen fills with messages, specify the /PAUSE option.
/SUB	Scans subdirectories inside a directory. By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories inside any directories you have specified. Do not use /SUB if you are scanning an entire drive.
/VIRLIST	Displays the name and a brief description of each virus that VirusScan detects. To pause when the screen fills with messages, specify the /PAUSE option. Use /VIRLIST alone or with /PAUSE on the command-line. You can save the list of virus names and descriptions to a file by redirecting the output of the command. For example, in DOS, enter: scan /virlist > filename.txt *Because VirusScan can detect many viruses, this file is more than 250 pages long*.

Type

Specifies the type of file that is infected (e.g., Executable, Word, Excel)

Location

Specifies the directory location of the infected file.

Size

Specifies the size of the infected file.

MS-DOS Name

Specifies the name of the infected file.

Created

Specifies the date the infected file was created.

Modified

Specifies the date the infected file was last modified.

Accessed

Specifies the date the infected file was last accessed.

Read-only

Specifies whether the file is read-only.

Hidden

Specifies whether the file is hidden.

Archive

Specifies whether the file is an archive file.

System

Specifies whether the file is a system file.

Program Files

Program files are file types which are most susceptible to virus infections. These include .COM, .EXE, .DO?, .XL?. To change which file types are scanned for viruses, complete the following procedure:

1 Click **Extensions**. The Program File Extensions dialog box is displayed.
2 To add a file extension to scan, click Add. Enter a new file extension and click **OK**. Repeat this step until all desired file extensions have been entered.
3 To delete an extension, select it and click Delete.
4 To return to the default extensions, click Default.
5 To exit without saving changes to the program files list, click cancel. To save the changes and exit, click **OK**.

Adding an exclude item

1 Enter the full path to a file, drive, or folder or click **Browse** to locate one.
2 To exclude subfolders from scanning, select the Include Subfolders checkbox.
3 To exclude the item from file scanning, select the File Scanning checkbox.
4 To exclude the item from boot sector scanning, select the Boot Sector Scanning checkbox.
5 To add the exclude item, click **OK**. To exit without adding the exclude item, click **Cancel**.

Notes

- To edit a scan item, select the item and click **Edit**.
- To remove a scan item, select the item and click **Remove**.

Adding a scan item

Select from the following:

- To scan all drives attached to this computer, click the Select Item to Scan option button and select My Computer.
- To scan all removable media, including floppy drives, click the Select Item to Scan option button and select All Removable Media.
- To scan all hard drives attached to this computer, click the Select Item to Scan option button and select All Fixed Disks.
- To scan all mapped network drives, click the Select Item to Scan option button and select All Network Drives.
- To scan an individual Drive or Folder, click the Select Drive or Folder to Scan option button and enter a path to the item to scan or click **Browse** to locate one.

After selecting a scan item, click **OK**. To exit without adding a scan item, click **Cancel**.

To change the password

1 Enter a new password.
2 Reenter the password.

Virus List

The Virus List helps you locate basic, but vital information about your virus. To find out about your virus, complete the following procedure:

Locate your virus by scrolling through the Virus List or clicking **Find Virus** and entering the virus name.

Highlight the virus and click **Virus Info**. The Virus Information page is displayed.

This information includes:

Virus Information, including:
Virus Name
Infects
Virus Size

Virus Characteristics, including:
Memory Resident
Encrypted
Polymorphic
Repairable
Macro Virus

Virus Information

This dialog box contains the following information:

Virus Information

Virus Name
Infects
Virus Size

Virus Characteristics

Memory Resident
Encrypted
Polymorphic
Repairable
Macro Virus

Item Information

This dialog box contains the following information:

Virus Name

File Information
Type
Location
Size

MS-DOS Name and Dates
MS-DOS Name
Created
Modified
Accessed

File Attributes
Read-only
Hidden
Archive
System

Opens the Add Scan Item dialog box where you can add an item to scan.

When enabled, the VShield task can be disabled from the taskbar or Console.

Closes the Virus Information Library.

Closes the Virus List.

Opens the Configuration property sheet where you can configure the task.

Indicates the date the file was created.

When enabled, a custom message will be displayed when a virus is detected.

Opens the Edit Scan Item dialog box where you can edit the currently selected scan item.

Enables the scheduler.

Indicates whether the virus is encrypted.

Opens the Add Exclude Item dialog box where you can add an Exclude item.

Lists items that are excluded from scanning.

Opens the Edit Exclude Item dialog box where you can edit the currently selected Exclude item.

Deletes the currently selected Exclude item.

Opens the Find Virus dialog box where you can find a virus by entering its name.

Indicates the types of files infected by this virus. These may include:
Executables (.EXE)
COM files (.COM)
Word files (.DO?)
Excel files (.XL?)

When enabled, any copies of this task will automatically be password protected.

When enabled, the size of the log file is limited.

When enabled, VShield automatically loads at startup.

When selected, infected file cleaning activity is logged.

When selected, scanning start times are logged.

When selected, infected file deletion activity is logged.

When selected, infected file detection activity is logged.

Opens the Browse dialog box where you can select a log file location.

When selected, infected file move activity is logged.

When selected, session settings are logged.

When selected, summaries of scan activity are logged.

When enabled, a virus activity log file is maintained.

When selected, the user name is logged.

Indicates whether the virus is a macro virus. Macro viruses infect Microsoft Word and Excel files.

Indicates whether the virus resides in memory.

Opens the Browse dialog box where you can select a quarantine location.

Enter a quarantine folder location.

Opens the Browse dialog box where you can select a server to receive Centralized Alerting messages.

Displays the next virus.

Enter any parameters required by the executable.

Indicates whether the virus is polymorphic. Polymorphic viruses modify their code to avoid detection.

Displays the previous virus.

Lists the path to the program executable.

Opens the Browse dialog box where you can locate the program's executable.

When enabled, the Clean Infected File option will be available on virus detection.

When enabled, the Continue Scanning (without taking any action) option will be available on virus detection.

When enabled, the Delete Infected File option will be available on virus detection.

When enabled, the Exclude option will be available on virus detection. This option is only recommended for false alarms.

When enabled, the Move Infected File option will be available on virus detection.

When enabled, the Stop Scan option will be available on virus detection.

Lists which property pages are protected. Protected pages are preceded by a  . Unprotected pages are preceded by a  .

Opens the Password dialog box where you can select a password.

Deletes the currently selected scan item.

Indicates whether the infected file can be cleaned.

Select whether the task will run minimized, maximized, or in a normal window.

Runs the task now.

Select how VirusScan or VShield responds to any infected files.

When selected, all file types are scanned. Although scanning all file types results in a thorough scan, scanning time will be significantly increased.

When selected, this task will scan for boot sector viruses.

When selected, compressed files are scanned.

Note

§ VirusScan's on-demand scanner scans PKZIP, PKLITE, WinZip, LZH and LZEXE files.
§ VShield scans PKLITE and LZEXE files

No help topic is associated with this item.

Opens the Program Files Extensions dialog box where you can select which file types are scanned for viruses. By default, COM files (.COM), executables (.EXE), Word files (.DO?), and Excel files (.XL?) are scanned.

Select an item to scan.

Opens the Browse dialog box where you can select a drive or folder to scan.

Lists currently configured scan items.

Opens a Browse dialog box where you can select a location to scan.

When selected, system memory is scanned before VirusScan begins scanning drives.

When selected, VShield scans for boot sector viruses on floppy access.

When selected, VShield scans for viruses when a file is copied.

When selected, VShield scans for viruses when a file is created.

When selected, VShield scans for viruses when a file is renamed.

When selected, VShield scans for viruses when a file is run.

When selected, VShield scans for boot sector viruses on system shutdown.

When selected, only file types that are susceptible to virus infection are scanned. To change which files types are scanned, click **Extensions**.

No help topic is associated with this item.

Select a drive or folder to scan or click Browse to locate one.

Indicates the task will run on the selected days at the specified time.

Select which day of the week the task will run.

Indicates the task will run on Friday at the specified time.

Indicates the task will run once an hour.

Indicates the task will run on Monday at the specified time.

Select which month the task will run.

Indicates the task will run once a month at the specified day and time.

Indicates the task will run once at the specified time and date.

Indicates the task will run on Saturday at the specified time.

Indicates the task will run on Sunday at the specified time.

Indicates the task will run on Thursday at the specified time.

Indicates the task will run on Tuesday at the specified time.

Indicates the task will run on Wednesday at the specified time.

Indicates the task will run weekly on the specified day and time.

Enables Centralized Alerting. Centralized Alerting is Network Associate's enterprise-wide virus notification solution. Once configured, workstations running VirusScan send virus notifications to servers running NetShield. This helps administrators locate the source of the virus infections and prevent them from spreading.

When enabled, the VShield icon is displayed on the taskbar.

When enabled, an audible alert will sound on detection of a virus.

When selected, this task automatically starts when opened.

Displays the executable's working directory.

Opens the Browse dialog box where you can select the executable's working directory.

Toggles the status bar on and off.

Indicates the number of infected files cleaned.

Indicates the number of infected files deleted.

Indicates the number of infected files found.

Indicates when the task was last started.

Indicates the number of infected files moved to a quarantine folder.

Specifies the next time the task will run.

Indicates the total number of files scanned.

When selected, all of the item's subfolders are scanned.

Displays the task name. To select a new name, enter a name and click Apply.

Toggles the title bar on and off.

Toggles the toolbar on and off.

No help topic is associated with this item.

Lists viruses. To find a specific virus, click Find Virus and enter the virus name or use the scroll bar.

Opens the Virus Information dialog box which contains information on virus characteristics.

Indicates the name of the virus.

Indicates the size of the virus.

Opens the Browse dialog box where you can select an item to exclude.

Enter the path to a drive, folder, or file to exclude.

When selected, the item's boot sector is not scanned.

When selected, the item's file(s) are not scanned.

When selected, the item's subfolders are not scanned.

Indicates when the file was last accessed.

Specifies whether the file is a archive file.

Specifies the files characteristics. These characteristics include whether the file is hidden, read-only, an archive file, or a system file.

Specifies when the file was created.

Indicates whether the file is hidden.

Specifies the file's location.

Specifies when the file was last modified.

Specifies the name of the file.

Indicates whether the file is a read-only file.

Specifies the size of the file.

Indicates whether the file is a system file.

Indicates the file type. The most commonly infected file types include: COM files, executables, Word files, or Excel files.

Lists virus characteristics.

Cleans the infected file.

Deletes the infected file.

Specifies the types of files this virus infects.

Opens the Browse dialog box so you can move the infected file to a quarantine location

Specifies the status of the infected file.

Specifies the name of the virus.

Specifies the size of the virus.

Enter a three-letter program file extension (e.g., .EXE, .COM).

Closes this page without applying any changes.

Closes this page.

Opens context-sensitive help for this page.

Applies any changes and exits this page.

Enter a password.

Reenter the password.

Enter the task's password.

Opens the Configuration property sheet where you can configure the task.

Starts this task.

Select a maximum log file size (in kilobytes).

Restores all scanning parameters to their default settings.

Starts scanning using the parameters you chose.

Halts scanning.

Select how many minutes after each hour this task will run.

Select which day of the week this task will run.

Select which day of the month the task will run.

Select which month the task will run.

Select which day of the week the task will run.

Lists the program file types checked for viruses.

Loads the default program file extensions list.

Opens the Add Program File Extension dialog box where you can add a new file extension.

Removes the selected extension.

Displays the name of the infected file.

Displays the name of the virus.

Applies any changes without exiting this page.

Stops this task.

Enables VShield.

Disables VShield.

Opens the Information property sheet which contains information on the virus and infected file.

Cleans the infected file.

Continues scanning without taking any action. When the scan is complete, you can manually respond to each infected file.

Deletes the infected file.

Continues scanning without taking any action and excludes this file from future scanning.

Note

§ This option is not recommended unless the file is generating a false alarm.

Moves the infected file to a quarantine folder.

Halts the scan and returns you to the main window.

Displays virus characteristics. These characteristics include whether the virus is memory-resident, encrypted, polymorphic, and whether the files it infects are repairable.

VirusScan for Windows Command-line Parameters

The following options are for use with VirusScan for Windows95, not with VirusScan for DOS. These options can be used as command-line parameters with shortcuts and icons to control the state of VirusScan when it is launched:

- **/NoSplash:** Suppresses the VirusScan splash screen
- **/AutoScan:** Starts scanning automatically

Desktop Management Interface

The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. The standard is independent of any particular operating system or protocol, and incorporates three layers:

- **Component Interface.** This layer offers a standard way for managed components such as application software, modems, hard disks, printers and other peripherals to describe their capabilities to a Service Provider. Most of the leading hardware manufacturers and many software vendors build component interface capability into their products and supply a description of their manageable attributes in a text file saved in Management Information Format (MIF).
- **Service Provider.** This layer collects information via the Component Interface from each component's MIF file, stores it in an MIF database, then formats and passes it upon request to desktop, local-area network, or console-based management applications. Each desktop computer has service provider code—often incorporated into the operating system—and its own MIF database.
- **Management Interface.** This layer offers a standard way for management applications to receive information about and to control desktop computers, their components, and their peripheral devices. Applications that support the Management Interface use it to interact with a desktop computer's Service Provider in order to send management requests in a standard format and receive system alerts and other information.

VirusScan can send virus alert messages to desktop and network management applications via the DMI Component Interface for easy retrieval and management.

Select this checkbox to configure VirusScan to send notifications to desktop or network management applications that support the Desktop Management Interface standard.

Select this checkbox to send notifications to desktop or network management applications that support the Desktop Management Interface standard.