Features of VirusScan

- NCSA-certified scanner assures detection of more than 90% of the viruses identified by the National Computer Security Association and 100% of the viruses found "in the wild." See the NCSA Website, www.NCSA.com, for certification status.
- 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 insert; system startup; and system shut down.
- On-demand scanning provides for user-initiated detection of known boot, file, mutation, multi-partite, stealth, encrypted, and polymorphic viruses located within files, drives, and diskettes.
- 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 subscription license to assure the best detection and removal rates. See Keeping VirusScan Updated.

See Also

About Viruses
Types of Viruses
Why Scan for Viruses
About Network Associates

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. And with outstanding support and anti-virus research from Network Associates teams worldwide, you can make sure your protection keeps up with the ever-changing computer world.

See Also

Features of VirusScan
Types of Viruses
Why Scan for Viruses?
About Network Associates

Types of Computer 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.

Boot Virus
File Virus
Stealth Virus
Multi-partite Virus
Mutating Virus
Encrypted Virus
Polymorphic Virus

See Also

About Viruses
Features of VirusScan
Why Scan for Viruses
About Network Associates

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 program 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.

Polymorphic Virus

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

Why Scan for Viruses?

In today's environment, safe computing practices are no longer a luxury—they are a necessity.
Computer viruses no longer attack your computing environment exclusively. They attack all computing environments you are in contact with through diskettes, networks, modems, and 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.

See Also

About Viruses
Features of VirusScan
Types of Viruses
About Network Associates

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 its network of authorized agent offices in more than 50 countries worldwide.

See Also

About Viruses
Features of VirusScan
Types of Viruses
Why Scan for Viruses

Removing 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. Begin the installation procedure described the VirusScan User's Manual.
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 Web Site related to manually removing viruses. For more information, see Contacting Network Associates.

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.

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, 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 100 per 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 your data files, take the following steps:

1. Download the data file (for example, DAT-9705.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 directory.
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 sites.
4. Locate the directories on the hard drive where VirusScan is currently loaded. Typically, the files are stored in C:\MCAFEE\VIRUSCAN.
5. Copy the new files into the directory or directories, overwriting the old data files.
   Some of the data files may be located in different directories. If so, place each updated file in its appropriate directory.
6. Reboot your computer so that changes take place immediately.

Notes

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 at least one year after your VirusScan purchase.

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.

Contacting Network Associates

Select from the following:

Customer Service
Technical Support
Training

Customer Service

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

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

See Also

Technical Support

Training

Technical Support

Network Associates is famous for its dedication to customer satisfaction. Network Associates has continued this tradition by investing considerable time and effort to make our website a valuable resource for updating Network Associates software and obtaining the latest news and information. For technical support information and issues, we encourage you to visit our website first.

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

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 NAI
America Online	Keyword NAI

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.

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

See Also

Customer Service
Training

Network Associates Training

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

See Also

Customer Service
Technical Support

Preventing Virus Infection

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.
To create a secure system environment and minimize your chance of infection, Network Associates recommends that you review the following topics:

Making an Emergency Diskette

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

To make a boot diskette, your system must be virus-free. Any virus residing in your system could be transferred to your boot diskette and reinfect your system. If your computer is infected, go to another computer, scan it, and if it is virus-free, complete one of the procedures below.

To make an Emergency Disk, select from the following:

Automatically Creating an Emergency Diskette
Manually Creating an Emergency Diskette

Automatically Creating an Emergency Diskette

To use VirusScan's utility for automatically creating an Emergency Disk, complete the following procedure:

1. Open the VirusScan program group and double-click the Create Emergency Diskette icon, or click-here.
2. Insert a blank 3.5" floppy disk into the A: drive.
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.

Manually Creating an Emergency Disk

Start this procedure from a command prompt (C:\>). If you are in Windows, you must open a DOS shell to get the prompt.

1. Insert a blank diskette in drive A:.
2. Format the diskette by typing the following command at the C:\> prompt:

   format a: /s /u

   This overwrites any information already on the diskette. If you are using DOS 5.0 or earlier, do not type the /u. If you are unsure of which version you are using, type ver at the C:\> prompt.
3. When the system prompts you for a volume label, enter an appropriate name using no more than eleven characters.
4. Change to the VirusScan directory.
5. Copy the command-line version of VirusScan to the diskette by typing the following commands at the prompt:

   copy scan.exe a:

   copy scan.dat a:

   copy clean.dat a:

   copy names.dat a:
6. Change back to the root directory by typing cd\.
7. Copy useful command-line programs to the diskette by typing one of the following commands at the C:\> prompt:

   copy c:\dos\chkdsk.* a:
8. Repeat the previous step for any other useful programs, including:

   debug.*
   diskcopy.*
   fdisk.*
   format.*
   label.*
   mem.*
   sys.*
   xcopy32.*
9. Label and write protect this diskette, then store it in a secure place. For more information, see Write Protecting a Diskette.

Note

If you use a disk compression utility, be sure to copy the drivers required to access the compressed drives onto the clean boot diskette. For more information about these drivers, see the documentation which accompanied the utility.

Write Protecting a Diskette

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.

Any diskettes that are not write protected should be scanned and cleaned before you write protect them.

Select from the following:

Write protecting 5.25" floppy diskettes
Write protecting 3.5" floppy diskettes

Write Protecting 5.25" Floppy Diskettes

1. Position the diskette face up with the label facing away from you.
2. The notch on the upper right hand side is called the write-protect notch. When this notch is visible, you can read and write data to and from the diskette. When the notch is covered with an adhesive tab, you can no longer write to the diskette. This prevents you from accidentally changing the data and prevents viruses from infecting the diskette.
3. To write protect the diskette, cover the notch with an adhesive tab or tape.

Write Protecting 3.5" Floppy Diskettes

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.
4. If there is no tab and the hole is open, the diskette is write protected.

Compressed Files

When enabled, VirusScan unpacks LZexe and PKLite compressed files and scans the decompressed form. Files with .ZIP and .LZH extensions are not scanned for viruses.

Move Infected Files

When this option is selected, VirusScan automatically moves infected files to the specified directory. To select a directory, enter the directory location or click **Browse** to select a directory.

After the file is moved to the quarantine directory, you can clean the file or restore the file from backups and return it to its original location. To return the file to the original directory location, refer to the VSHIELD log file (VSHLOG.TXT) or the VirusScan On-demand Scanning log file (VSCLOG.TXT).

Clean Infected Files

When this option is selected, VirusScan will automatically attempt to remove the virus from the infected file.

Delete Infected Files

When this option is selected, VirusScan will automatically delete infected files. 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, VirusScan continues scanning without taking any action. When the scan is complete, you can manually respond to each infected file in the VirusScan Main Window.

This option is not recommended for unattended machines.

Prompt for Action

When this option is selected, VirusScan will prompt you for action for each infected file.

Safe Computing Practices

Safe computing practices include:

Virus protection
Regular backups
Meaningful password protection
Training and awareness

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 directory.
2. Make sure you have rights to this directory.
3. Configure VShield and VirusScan tasks to send network messages to this directory.

Program Files

To add or remove file types from the program files list, click **Extensions**. The Program File Extensions dialog box is displayed.

1. To add a file extension, click **Add**. Enter a new file extension to scan and click **OK**. Repeat this procedure until all desired file extensions are entered.
2. To delete an extension, select it and click **Delete**.
3. To return to the default extensions, click **Default**.

When you are finished editing the list of file extensions, click **OK**.

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 (.XLS)

Virus Size

Indicates the size of the virus in kilobytes.

Memory Resident

Indicates whether the virus resides in memory.

Encrypted

Indicates whether this is an encrypted virus.

Polymorphic

Indicates whether this is an polymorphic virus.

Repairable

Indicates whether files infected by this virus are repairable.

Macro Virus

Indicates whether this is a Word or Excel macro virus.

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.

VirusScan DOS Error Levels

When you run VirusScan in the DOS environment, 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:

ERRORLEVEL	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, directory, 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.)

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 a VSC file, open it with any text editor.

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

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 inside compressed files Default value: 1
szProgramExtensions	Type: String Defines extensions to be scanned Default value: EXE COM DO? XL?
szDefaultProgram Extensions	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) Instructs VirusScan to send a Centralized Alerting notification to a server running NetShield. Default value: 0
szNetworkAlertPath	Type: String Defines the path to the server running NetShield. Default value: none
bSoundAlert	Type: Boolean (1/0) Instructs VirusScan to sound an alert when a virus is detected Default value: 1

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: 1 - Prompt for action 2 - Move infected files to a folder 3 - Clean infected files automatically 4 - Delete infected files automatically 5 - Continue scanning Default value: 2
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: 1
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: Your custom message

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 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
bLogSetting	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
szScanItem_0	Type: String Defines item to be scanned Default value: C:\

SecurityOptions

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

	Default value: 0
szPasswordCRC	
bInheritSecurity	

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 2 - Instructs VShield to not exclude subfolders

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, open it with any text editor.

Note

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
bLoadAtStartup	Type: Boolean (1/0) Defines if VShield should be loaded at system startup Default value: 1
bNoSplash	Type: Boolean (1/0) Instructs VShield to not show splash screen when program is launched Default value: 0

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 inside 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) Instructs VirusScan to send a Centralized Alerting notification to a server running NetShield. Default value: 0
szNetworkAlertPath	Type: String Defines the path to the server running NetShield 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 the 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 the 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 the 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 without taking action 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: Your custom message

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\VShield Activity Log.txt

SecurityOptions

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

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 2 - 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	
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.

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.

Macros, below

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 most current version of the Virus Information Library, navigate to http://www.nai.com/ /vinfo

Emergency Disk Creation Utility

Please wait while the Emergency Disk creation utility loads.

Note

If this takes more than a few seconds, please start the Emergency Disk creation utility manually. To start the utility manually, open the VirusScan program group and double-click the Create Emergency Disk icon.

VShield Properties

Please wait while the VShield loads.

Note

If this takes more than a few seconds, please start the VShield manually. To start the VShield manually, open the VirusScan program group and double-click the VShield icon.

VirusScan Console

Please wait while the VirusScan Console loads.

Note

If this takes more than a few seconds, please start the VirusScan Console manually. To start the VirusScan Console manually, open the VirusScan program group and double-click the VirusScan Console icon.

VirusScan's On-Demand Scanner

Please wait while VirusScan loads.

Note

If this takes more than a few seconds, please start VirusScan manually. To start VirusScan manually, open the VirusScan program group and double-click the VirusScan icon.

NCSA Website

Please wait while we access the NCSA Website.

Note

To access the NCSA Website, 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 have access to the World Wide Web, you can access the website at http://www.ncsa.com.

Adobe Website

Please wait while we access the Adobe Website.

Note

To access the Adobe Website, 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 have access to the World Wide Web, you can access the website at http://www.adobe.com.

VShield Virus Activity Log

Please wait while the activity log loads.

Note

If the activity log does not open, either the Log to File option is not active or you are not using the default log file name. To manually open the VShield activity log, simply open the file defined on the Report page with any text editor (e.g., Notepad, Word, etc.).

On-demand Scanning Virus Activity Log

Please wait while the activity log loads.

Note

If the activity log does not open, either the Log to File option is not active or you are not using the default log file name. To open the activity log, select View Activity Log from the File menu.

Virus List

Please wait while the Virus List loads.

Note

If this takes more than a few seconds, please open the Virus List manually. To open the Virus List manually, start the File Manager, navigate to the VirusScan directory, and double-click VIRLST16.EXE.

end macros

VirusScan User's Manual

The VirusScan User's Manual is in the Adobe Acrobat format (PDF) and is available on the VirusScan CD-ROM. To open the VirusScan User's Manual, start Adobe Acrobat and open the WSCDOC31.PDF.

Note

You must have the Adobe Acrobat Reader installed to view the manual. The Acrobat reader is available on the CD-ROM version of this product or can be downloaded from www.adobe.com. To access the Adobe Website, click here.

Context-sensitive, below

Program Files

1. To add a file extension, click **Add**.
2. Enter a new file extension to scan and click **OK**.
3. Repeat Steps 1 and 2 until all desired file extensions are entered.
4. When you are finished editing the list of file extensions, click **OK**.

Tips

To delete an extension, select it and click **Delete**.
To return to the default extensions, click **Default**.

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 mounted network drives, click the Select Item to Scan option button and select All Network Drives.
- To scan an individual drive or directory, click the Select Drive or Directory 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**.

Adding an exclude item

1. Enter the full path to a file, drive, or directory or click **Browse** to locate one.
2. To exclude subdirectories from scanning, select the Include Subdirectories 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**.

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:

1. Locate your virus by scrolling through the Virus List or clicking **Find Virus** and entering the virus name.
2. Highlight the virus and click **Virus Info**. The Virus Information page is displayed.
3. 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