Detection Page

The Detection page is used to configure which file locations and file types are scanned. To configure the Detection page, complete the following procedure:

1 Open the VShield Configuration Manager. The VShield Configuration Manager opens with the Detection page displayed.
2 Select when VShield scans files for viruses. VShield can check for viruses when files are run, copied, created, or renamed.
3 Select when VShield floppy disks for viruses. VShield can check floppies on access or shutdown.
4 To scan all file types for viruses, select the All Files checkbox. To only scan files that are most susceptible to viruses, select the Program Files Only option button. To change which file types are included in the Program Files list, click **Extensions**.
5 To scan compressed files, select the Compressed Files checkbox.
6 To configure VShield to load at system startup, select the Load VShield at Startup checkbox.
7 To allow VShield to be disabled, select the VShield can be disabled checkbox.
8 To show the VShield icon on the taskbar, select the Show VShield Icon on Desktop checkbox.
9 To save the changes and continue configuring VShield, click **Apply** and select another property page. To save the changes and exit, click **OK**. To exit without saving the changes, click **Cancel**.

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

Action page

The Action page is used to configure how VShield responds to any infected file(s). To configure the Action page, complete the following procedure:

1 Open the VShield Configuration Manager. The VShield Configuration Manager opens with the Detection page displayed.

2 Click the Action tab.

3 Select how VShield will respond to any infected file(s).
Prompt for action
Move infected files to a directory
Clean infected files
Delete infected files
Continue Scanning

4 To save the changes and continue configuring VShield, click **Apply** and select another property page. To save the changes and exit, click **OK**. To exit without saving the changes, click **Cancel**.

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

Alert page

1 Open the VShield Configuration Manager . The VShield Configuration Manager opens with the Detection page displayed.
2 Select the Alert tab.
3 To configure VShield to send a network message, select the Send Network Alert checkbox. Enter a user name or click Browse to locate a user.
4 To configure VShield to sound an audible alert, select the Sound Audible Alert checkbox.
5 To configure VShield to send a custom message, select the Display Custom Message checkbox and enter a custom message (up to 256 characters).
6 To save the changes and continue configuring VShield, click **Apply** and select another property page. To save the changes and exit, click **OK**. To exit without saving the changes, click **Cancel**.

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

Report page

1 Open the VShield Configuration Manager . The VShield Configuration Manager opens with the Detection page displayed.
2 Click the Reports tab.
3 For VShield to send you a message each time a virus is encountered, select the Display Message checkbox and enter a message.
4 For VShield to sound an audible alert, select the Sound Alert checkbox.
5 For VShield to maintain a log file, select the Log to File checkbox. Enter a path and filename for the log file (default: C:\Program Files\McAfee\VirusScan\VSLOG.TXT).
6 To limit the size of the log file, select the Limit Size of Log File checkbox and enter the maximum log file size.
7 Select which items VShield will log in the What to Log section.
8 To save the changes and continue configuring VShield, click **Apply** and select another property page. To save the changes and exit, click **OK**. To exit without saving the changes, click **Cancel**.

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

Exclusion page

1 Open the VShield Configuration Manager. The VShield Configuration Manager opens with the Detection page displayed.
2 Select the Exclusions tab.
3 To add an item to exclude from scanning, click Add. The Exclude Item dialog box is displayed.

   Enter the full path to a file, drive, or directory or click Browse to locate one.

   To exclude subdirectories from scanning, select the Include Subdirectories checkbox.

   To exclude the item from file scanning, select the File Scanning checkbox. To exclude the item from boot sector scanning, select the Boot Sector Scanning checkbox.
4 Repeat Step 3 for each exclusion item.
5 To edit a scan item, select the item and click Edit.
6 To remove a scan item, select the item and click Remove.
7 To save these changes to the default scanning profile, select Save As Default.
8 To save the changes and continue configuring VShield, click **Apply** and select another property page. To save the changes and exit, click **OK**. To exit without saving the changes, click **Cancel**.

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

Security page

1 Open the VShield Configuration Manager . The VShield Configuration Manager opens with the Detection page displayed.
2 Select the Security tab.
3 Select which property pages to protect. Protected pages are preceded by a  . Unprotected pages are preceded by a  .
4 Click **Password**. The Specify Password dialog box is displayed.
5 Enter a password, reenter the password, and click OK. You are returned to the Password Protection dialog box.
6 To save the changes and continue configuring VShield, click **Apply** and select another property page. To save the changes and exit, click **OK**. To exit without saving the changes, click **Cancel**.

Notes

- Passwords are not case-sensitive. For example, if you chose the password, "VirusScan"; "VIRUSSCAN", "virusscan", and even "ViRuSsCaN" would be accepted.
- Whenever anyone attempts to access one of the protected pages, they will be prompted for a password.
- You are prompted for a password once per session.

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

Responding to a Virus

Viruses attack computer systems by infecting files—usually executable program files or Microsoft Word documents and templates. VShield can safely remove most viruses from infected files and repair any damage. Some viruses, however, are designed to damage your files beyond repair. These irreparably damaged files, called “corrupted” files, can be moved by VShield to a quarantine directory or deleted to prevent another virus infection of your system.

If VShield finds infected files, complete one of the following procedures:

{button ,JI(`vshcfg32.HLP',`Responding_to_a_virus_found_in_a_file')} Removing a virus found in a file

{button ,JI(`vshcfg32.HLP',`Responding_to_a_virus_found_in_memory')} Removing a virus found in memory

Responding to a virus found in a file

If VShield detects a virus in a file, it will take the action you specified during configuration. See Action property page.

{button ,JI(`vshcfg32.HLP',`Removing_a_Virus_Prompt_for_Action')} Prompt for Action
{button ,JI(`vshcfg32.HLP',`Removing_a_Virus_Move_Infected_Files_to_a_Directory')} Move infected files to a directory
{button ,JI(`vshcfg32.HLP',`Removing_a_Virus_Clean_Infected_Files')} Clean infected files
{button ,JI(`vshcfg32.HLP',`Removing_a_Virus_Delete_Infected_Files')} Delete infected files
{button ,JI(`vshcfg32.HLP',`Removing_a_Virus_Continue_Scanning')} Continue scanning

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

Prompt for Action

If you selected Prompt for Action from the Action property page and VShield finds a virus, the Virus Found screen is displayed.

Select one of the following options:

{button ,JI(`vshcfg32.HLP>more',`Prompt_for_Action_Continue')} Continue
{button ,JI(`vshcfg32.HLP>more',`Prompt_for_Action_Stop')} Stop
{button ,JI(`vshcfg32.HLP>more',`Prompt_for_Action_Clean')} Clean
{button ,JI(`vshcfg32.HLP>more',`Prompt_for_Action_Delete')} Delete
{button ,JI(`vshcfg32.HLP>more',`Prompt_for_Action_Exclude')} Exclude

Move Infected Files to a Directory

If you selected Move Infected Files from the Action property page and a virus is found, the infected file will automatically be copied to the specified 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 help you locate the source of the infection, the path to infected file is duplicated in the quarantine directory. For example, if an infected file was found in C:\WINDOWS\SYSTEM and you specified C:\INFECTED as the quarantine directory, it would be copied to C:\ INFECTED \WINDOWS\SYSTEM.

Clean Infected Files

If you selected Clean Infected Files from the Action property page and a virus is found, VShield will automatically attempt to clean the file.

Note

- If the virus was not successfully cleaned, VShield will prompt you to choose another action. Select Delete and restore the file from backup.

Delete Infected Files

If you selected Delete Infected Files from the Action property page and a virus is found, VShield will automatically delete the infected file.

Note

- If this option is selected, confirm that report logging is enabled. This will ensure you have a record of which files were deleted, so you can restore them from backups. See Reports.

Continue Scanning

If you selected Continue Scanning from the Action property page and a virus is found, VShield will continue scanning without taking any action.

Note

- This option is not recommended.

Prompt for Action: Continue

VShield continues scanning without taking any action.

Note

- This option is not recommended.

Prompt for Action: Stop

Halts the scan and returns you to the main window.

Prompt for Action: Clean

VShield attempts to clean the file.

Note

- If the virus was not successfully cleaned, VShield will prompt you to choose another action. Select Delete and restore the file from backup.

Prompt for Action: Delete

VShield deletes the infected file.

If this option is selected, confirm that report logging is enabled. This will ensure you have a record of which files were deleted, so you can restore them from backups. See Reports.

Prompt for Action: Exclude

Excludes the file from future scanning.

To open the VShield Configuration Manager

Click Start, point to Programs, point to McAfee VirusScan, and click VShield Configuration Manager.

Tip

- To quickly open the VShield Configuration Manager, right-click the VShield icon () on the taskbar and select Properties from the Shortcut menu.

Context-sensitive, below

Detection Page

The Detection page is used to configure which file locations and file types are scanned. To configure the Detection page, complete the following procedure:

1 Select when VShield scans files for viruses. VShield can check for viruses when files are run, copied, created, or renamed.

2 Select when VShield floppy disks for viruses. VShield can check floppies on access or shutdown.

3 To scan all file types for viruses, select the All Files checkbox. To only scan files that are most susceptible to viruses, select the Program Files Only option button. To change which file types are included in the Program Files list, click **Extensions**.

4 To scan compressed files, select the Compressed Files checkbox.

5 To configure VShield to load at system startup, select the Load VShield at Startup checkbox.

6 To allow VShield to be disabled, select the VShield can be disabled checkbox.

7 To show the VShield icon on the taskbar, select the Show VShield Icon on Desktop checkbox.

8 To save the changes and continue configuring VShield, click **Apply** and select another property page. To save the changes and exit, click **OK**. To exit without saving the changes, click **Cancel**.

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

Action page

The Action page is used to configure how VShield responds to any infected file(s). To configure the Action page, complete the following procedure:

1 Select how VShield will respond to any infected file(s).
   Prompt for action
   Move infected files to a directory
   Clean infected files
   Delete infected files
   Continue Scanning
2 To save the changes and continue configuring VShield, click **Apply** and select another property page. To save the changes and exit, click **OK**. To exit without saving the changes, click **Cancel**.

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

Alert page

1 To configure VShield to send a network message, select the Send Network Alert checkbox. Enter a user name or click Browse to locate a user.
2 To configure VShield to sound an audible alert, select the Sound Audible Alert checkbox.
3 To configure VShield to send a custom message, select the Display Custom Message checkbox and enter a custom message (up to 256 characters).
4 To save the changes and continue configuring VShield, click **Apply** and select another property page. To save the changes and exit, click **OK**. To exit without saving the changes, click **Cancel**.

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

Report page

1 For VShield to send you a message each time a virus is encountered, select the Display Message checkbox and enter a message.
2 For VShield to sound an audible alert, select the Sound Alert checkbox.
3 For VShield to maintain a log file, select the Log to File checkbox. Enter a path and filename for the log file (default: C:\Program Files\McAfee\VirusScan\VSLOG.TXT).
4 To limit the size of the log file, select the Limit Size of Log File checkbox and enter the maximum log file size.
5 Select which items VShield will log in the What to Log section.
6 To save the changes and continue configuring VShield, click **Apply** and select another property page. To save the changes and exit, click **OK**. To exit without saving the changes, click **Cancel**.

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

Exclusion page

1 To add an item to exclude from scanning, click Add. The Exclude Item dialog box is displayed.
2 Enter the full path to a file, drive, or directory or click Browse to locate one.
3 To exclude subdirectories from scanning, select the Include Subdirectories checkbox.
4 To exclude the item from file scanning, select the File Scanning checkbox. To exclude the item from boot sector scanning, select the Boot Sector Scanning checkbox.
5 Repeat Step 1-4 for each exclusion item.
6 To save these changes to the default scanning profile, select Save As Default.
7 To save the changes and continue configuring VShield, click **Apply** and select another property page. To save the changes and exit, click **OK**. To exit without saving the changes, click **Cancel**.

Tips

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

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

Security page

1 Select which property pages to protect. Protected pages are preceded by a  . Unprotected pages are preceded by a  .

2 Click **Password**. The Specify Password dialog box is displayed.

3 Enter a password, reenter the password, and click OK. You are returned to the Password Protection dialog box.

4 To save the changes and continue configuring VShield, click **Apply** and select another property page. To save the changes and exit, click **OK**. To exit without saving the changes, click **Cancel**.

Notes

- Passwords are not case-sensitive. For example, if you chose the password, "VirusScan"; "VIRUSSCAN", "virusscan", and even "ViRuSsCaN" would be accepted.
- Whenever anyone attempts to access one of the protected pages, they will be prompted for a password.
- You are prompted for a password once per session.

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

Adding an exclude item

1 Enter the full path to a file, drive, or directory 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**.

To change the password

1 Enter a new password.
2 Reenter the password.

Using the VirusScan Console

The VirusScan Console configures VShield and schedules and configures on-demand tasks.

Click here  to start the VirusScan Console.

Tip

- To start VirusScan from the desktop, click Start, point to Programs, point to McAfee VirusScan, and click VirusScan Console.

Using VirusScan's on-demand scanner

VirusScan's on-demand scanner, provides for user-initiated detection of both known and unknown viruses.

Click here  to start VirusScan's on-demand scanner.

Tip

- To start VirusScan from the desktop, click Start, point to Programs, point to McAfee VirusScan, and click VirusScan.

Using VShield, VirusScan's on-access Scanner

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.

Click here  to configure VShield.

Tip

- To configure VShield from the desktop, click Start, point to Programs, point to McAfee VirusScan, and click VShield Configuration Manager.

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.
- Scan, VirusScan's on-demand scanner, provides for user-initiated detection of known boot, file, mutation, multi-partite, stealth, encrypted, and polymorphic 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 McAfee's proprietary 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 McAfee subscription license to assure the best detection and removal rates. See Keeping VirusScan Updated.

What is a Computer Virus?

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

McAfee's 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.

Components of VirusScan

(New topic text goes here.)

About McAfee

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

McAfee does not stop at developing the world's best anti-virus and utility products. We back them with the industry's best service and technical support. Product support is provided by a full-time staff of virus researchers, programmers, and support professionals and delivered directly by McAfee or our network of authorized agent offices 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 McAfee 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 McAfee Web Site related to manually removing viruses. For more information, see Contacting McAfee.

{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, McAfee 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.

McAfee's 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(`vs-main.HLP>(w95sec)',`Updating_VirusScan_using_Electronic_Update')} Electronic Update

{button ,JI(`vs-main.HLP>(w95sec)',`Updating_VirusScan_manually')} Manual Update

Note

- McAfee 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.

Updating VirusScan using Electronic Update

McAfee's new feature, Electronic Update, 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-9609.ZIP) from one of McAfee's 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 McAfee electronic sites.
4 Locate the directories on the hard drive where VirusScan is currently loaded. Typically, the files are stored in C:\Program Files\McAfee\VirusScan95.

Tip

- To access the McAfee 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 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 an Emergency Disk, complete the following procedure:

1. 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.
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.

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 clean boot diskette. For more information, see the documentation which accompanied those utilities.

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.

Select from the following:

{button ,JI(`vs-main.HLP>(w95sec)',`Write_protecting_a_3.5_floppy_disk')} 3.5" Diskettes

{button ,JI(`vs-main.HLP>(w95sec)',`Write_protecting_a_5.25_floppy_disk')} 5.25" Diskettes

Note

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

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.

Note

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

To write-protect a 5.25" floppy disk

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.

Contacting McAfee

Select from the following:

{button ,JI(`vs-main.HLP',`Customer_Service')} Customer Service

{button ,JI(`vs-main.HLP',`Technical_Support')} Technical Support

{button ,JI(`vs-main.HLP',`McAfee_Training')} 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:

McAfee, Inc.
2710 Walsh Avenue
Santa Clara, CA 95051-0963
U.S.A.

Technical Support

McAfee is famous for its dedication to customer satisfaction. McAfee has continued this tradition by investing considerable time and effort to make our website a valuable resource for updating McAfee 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.mcafee.com

Click here  to access the McAfee Website.

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

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

If the automated services did not solve your problem, you may contact McAfee 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

McAfee Training

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

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:

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, 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.)

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.

To help you locate the source of the infection, the path to infected file is duplicated in the quarantine directory. For example, if an infected file was found in C:\WINDOWS\SYSTEM, it would be copied to C:\QUARANTINE\WINDOWS\SYSTEM.

Clean Infected Files

When this option is selected, viruses are automatically remove 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.

Program Files is also context-sensitive

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** or **Program Files**. 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 are 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 unpacks LZexe and PKLite compressed files and scans the decompressed form. Files with .ZIP and .LZH extensions are not scanned for viruses.

McAfee Virus Information Library

Click here  to open the McAfee Virus Information Library.

Note

- If the Library takes more than 10-15 seconds to load, it may not be installed on your system. To install the Virus Information Library, simply copy the file MCAFEE.HLP to your VirusScan directory (default C:\Program Files\McAfee\VirusScan).
- To start the Virus Information Library manually, open the Windows Explorer and double-click the MCAFEE.HLP help 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.

DetectionOptions

Variable	Description
szProgramExtensions	Type: String Defines extensions to be scanned Default value: EXE COM DO?
szDefaultProgramExtensions -	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: EXE COM DO?
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 (PkLite, LZEXE) Default value: 0

ActionOptions

Variable	Description
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
szMoveToFolder	Type: String
	Defines folder to which infected files should be moved
	Default value: \Infected
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
Variable	Description
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
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
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
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

ReportOptions

Variable	Description
szLogFileName	Type: String Defines log file name Default value: C:\Program Files\McAfee\VShield Activity Log.txt
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

General

Variable	Description
bLoadAtStartup	Type: Boolean (1/0) Defines if VShield should be loaded at system startup Default value: 1
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
bNoSplash	Type: Boolean (1/0)
	Instructs VShield to not show splash screen when program is launched
	Default value: 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
	2 - 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
szProgramExtensions	Type: String Defines extensions to be scanned Default value: COM DO? EXE
szDefaultProgramExtensions	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: COM DO? EXE
szMoveToFolder	Type: String Defines folder to which infected files should be moved Default value: \Infected
bIncludeSubFolders	Type: Boolean (1/0) Instructs VirusScan to search for viruses inside subfolders Default value: 1
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
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
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
szScanItem	Type: String Defines item to be scanned Default value: C:\

AlertOptions

Variable	**Description**
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection Default value: Your custom message
szSuggestMessage	Type: String Instructs VirusScan to display this message in place of the McAfee suggested message in the prompt display box Default value: Your custom message
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed upon virus detection Default value: 0
bSoundAlert	Type: Boolean (1/0) Instructs VirusScan to sound an alert when a virus is detected

	Default value: 1
Variable	**Description**
szLogFileName	Type: String Defines log file name Default value: VSLOG.TXT
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