About VirusScan 95

McAfee's VirusScan 95 program detects, identifies, and disinfects known DOS and Windows computer viruses. VirusScan 95 checks memory as well as both the system and data areas of disks for virus infections. If VirusScan 95 finds a known virus, in most cases it will eliminate the virus and fully repair infected programs or system areas to their original condition.

VirusScan 95 is designed to check for pre-existing infections of known and unknown viruses on floppy, hard, CD-ROM, and compressed (DriveSpace, SuperStor, Stacker, DoubleSpace, etc.) disks on both stand-alone and networked personal computers, as well as network file servers. If you have a Novell NetWare/386 V3.1x or 4.xx file server, use the NetShield virus prevention software NetWare Loadable Module in conjunction with VirusScan 95.

What is a computer virus?

A computer virus is a software program that attaches itself to another program in computer memory or on a disk, and spreads from one program to another. Viruses can damage data, cause computers to crash, display offending or bothersome messages, or lie dormant until such time they are set to "awaken."

Why do I need to scan for viruses?

In today's industry, scanning is no longer considered to be an extravagance - but a necessity. Computer viruses no longer attack your computing environment but all other computing environments which you contact. Computer viruses can attach and later propagate themselves through disks and files. Important information and hardware losses could plague your computing environment should you not take the proper precautions. McAfee's anti-virus line of products heads up the list of proper precautions. Scheduled periodic scans of your computing environment can offer you that added assurance that you are practicing "safe computing."

To configure a Scan

1. Select the **Where & What** tab.
2. Enter a path in the **Scan in** field or click **Browse** to select the desired location.
3. Select the desired radio button and check boxes.

Tip

- To get information on a control, click the right mouse button.

{button ,KL("Scan;Options")} Related Topics

To select Actions

1. Select the **Actions** tab.
2. Select an Action from the provided list box.

Tips

- Make regular backups and keep original diskettes for all your applications.
- If you do not keep backups of your programs, do not select automatic virus removal.

{button ,KL("Scan;Options")} Related Topics

To report Scan Results

1. Select the **Reports** tab.
2. Select the **Display message** check box and enter a message in the provided text box.
3. Select the **Sound alert** check box to be notified by an electronic beep when VirusScan is complete and a virus is detected.
4. Select the **Log to File** check box and enter a log file name in the provided text box or click **Browse** to locate the desired file.
5. To limit the log file size, select the corresponding check box and enter a value between 10 and 999 K in the provided field.

Tips

- To view or print a log file, launch notepad.
- An unlimited log file size can take up valuable disk space.
- The log file is appended when viruses are found.

{button ,KL("Scan;Options")} Related Topics

To initiate Scanning from the Scan window

1. Select the **Where & What** tab.
2. Specify the desired path and file options.
3. Select the **Actions** tab.
4. Specify the desired action.
5. Select the **Reports** tab.
6. Specify the desired reporting options.
7. Click **Scan Now**.

Tips

- To terminate scanning, click **Stop**.
- Scan can be launched in multiple instances to accommodate the need to scan more than one location or file. Just highlight multiple Drives or Folders, right mouse click, and select Scan for Viruses.

{button ,KL("Scan;Options")} Related Topics

To initiate a Scan from the Context Menu

1. Click the right mouse button on the desired Directory or Drive icon to display the context menu.
2. Choose **VirusScan** from the context menu.
3. Select the desired options from the provided tabs.
4. Click **Scan Now**.

To initiate a Scan from the StartUp of Windows

1. Launch Scan.
2. Select the desired options from the provided tabs.
3. Choose **Save Settings** from the **File** menu.
4. Save the settings file to the StartUp Folder.

Tips

- To rename a Settings file from within Explorer, select the desired file and choose File | Rename.
- To launch Scan from within Explorer, double click on a Settings file.
- The StartUp folder is typically located under C:\WINDOWS\Start Menu\Programs.

{button ,KL("Options")} Related Topics

To clean files automatically

1. Select the Actions tab.
2. Choose **Clean infected files** from the **When virus is found** list box.
3. Click **Scan Now**.

Note: This procedure is *not* recommended for those environments which are not backed up on a regular basis.

Tips

- To delete infected files, choose **Delete infected files**.
- To be prompted upon virus detection, choose **Prompt for action**.
- To clean virus from the Infected File Info dialog, choose **Prompt for action**.

{button ,KL("Options")} Related Topics

To clean infected files from a Scan prompt

1. Select the **Actions** tab.
2. Choose **Prompt for action** from the **When virus is found** list.
3. Click **Scan Now**.
4. When virus is found, click **Clean**.

Tips

- To display information about the virus, double click on the file name in the list of infected files.
- Most infected file operations can be performed by clicking right mouse button on the infected file.

{button ,KL("Scan;Options")} Related Topics

About McAfee

Founded in 1989, McAfee Inc. is the leading provider of productive computing tools for DOS, OS/2, 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 can be purchased through dealers or downloaded from bulletin board systems and on-line services around the world.

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

Before you contact McAfee

Have the following information ready:

{button ,PI("","IDH_PROGNAME")} Program name and version number

{button ,PI("","IDH_PCBRAND")} Type and brand of computer, hard disk and any peripherals

{button ,PI("","IDH_HOWTOMSD")} Version of Windows, along with any TSRs or device drivers in use

{button ,PI("","IDH_HOWTOMSD")} Printouts of your AUTOEXEC.BAT and CONFIG.SYS files

{button ,PI("","IDH_HOWTOMSD")} A printout of the contents of memory, from the MSD command

{button ,PI("","IDH_HOWTOSENDINFO")} A description of the exact problem you are having. Please be as specific as possible. If you cannot be at your computer when you call, a printout of the screen will be helpful.

Tips

- You can also gather system information by using Device Manager.

Contacting McAfee

Phone (408) 988-3832
Monday through Friday
6:00 a.m. to 5:00 p.m. Pacific Standard Time

Fax (408) 970-9727

Mail McAfee, Inc.
2710 Walsh Avenue
Suite 200
Santa Clara, CA 95051

Modem McAfee Bulletin Board System (BBS) (24 hours)
CompuServe
Internet
America Online

Preventing viruses

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

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

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

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

Use software only from reputable sources

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

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

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

Scan all incoming disks and files for viruses

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

{button ,KL("Making regular backups")} Related Topics

Making regular backups

Some viruses may leave certain disks or files unusable even after they are cleaned. Between 10% and 20% of all infections involve files that are corrupted beyond repair.

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

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

{button ,KL("Preventing viruses")} Related Topics

To Save Settings

1. Select desired settings in the provided tabs.
2. Choose **Save Settings** from the **File** menu.

Tips

- To rename a Settings file from within Explorer, select the desired file and choose Rename from the File menu.
- To launch VirusScan from within Explorer, double click on a Settings file.
- To initiate a scan from login, copy or save a Settings file into your StartUp folder.

{button ,KL("Options")} Related Topics

To print Log Files

Do one of the following to print a log file:

- Launch Notepad and open desired log file

  or

- Double click on the desired log file icon in Explorer

Tips

- Log files can be viewed or printed from the context menu.

What to do if Scan found a virus

1. **Do not panic!**
2. **Do not run any other programs.**
3. Start a scan with **Prompt for action** or **Clean infected files** action.
4. If Scan is unable to remove a virus, delete the infected file and reinstall it.

- If you are at all unsure about how to proceed once you have found a virus, contact McAfee Technical Support.

Tip

- We strongly recommend that you get experienced help in dealing with viruses if you are unfamiliar with anti-virus software and methods. This is especially true for critical viruses, master boot record (MBR), and boot sector infections because improper removal of these viruses can result in the loss of all data and use of the infected disks.

{button ,KL("Restore deleted file")} Related Topics

What to do if Scan deleted an infected file

- Restore file from backup,
  or
- Reinstall program containing deleted file from a set of virus free installation diskettes.

{button ,KL("Making regular backups")} Related Topics

Command line Options

Option	Description
/AUTOSCAN	Starts scanning immediately after launch
/NOSPLASH	Disables display of the splash screen

Other McAfee Products

Protects your valuable files with the most rigorous and thorough virus protection in the world.

The world's best anti-virus utility for Novell file servers.

Centrally Controls and Manages Windows on Networks.

Empowers you to effectively manage and control software.

True enterprise metering of LAN applications.

Program name, version and serial number can be obtained from the About {Product Name} dialog. Choosing Help |About displays the product-specific dialog.

Brand and model of your computer can be found in your User's Manual or on the back panel of the computer.

Launching MSD

1. Choose Start | Run.
2. Type MSD in the provided text box.
3. Choose OK.

The MSD console is displayed.

4. Select File | Print Report.
5. Select the Report All check box.
6. Select the Print to file check box and enter a file name in the provided text box.
7. Choose File | Exit to return to your desktop.

Information about your computer and the product can be sent to McAfee by mail, fax or modem.

Contact McAfee's electronic Bulletin Board System (BBS) at (408) 988-4004.

Our multi-line BBS is accessible 24 hours a day, 365 days a year, except for scheduled downtime and maintenance. All lines run high-performance modems operating from 1,200 bps to 28,800 bps with line settings of 8 data bits, no parity, and 1 stop bit.

People or organizations authorized to provide service, sales, and support for McAfee products in 50+ countries around the world.

See AGENTS.TXT for a current list of McAfee agents.

We sponsor the McAfee Virus Help Forum on CompuServe. To access, type `GO MCAFEE` at any CompuServe prompt. A free introductory membership is available through CompuServe.

The latest versions of McAfee's anti-virus software are available by anonymous ftp (file transfer protocol) over the Internet at **ftp.mcafee.com**. If your domain resolver does not support names, use the IP# 192.187.128.3. Enter **anonymous** or **ftp** as your user ID and your own e-mail address as the password. Programs are located in the pub/antivirus directory. If you have questions, please send e-mail to **support@mcafee.com**.

You can also find McAfee's anti-virus software at the Simtel Software Repository at **Oak.Oakland.EDU** in the **pub/msdos/virus** directory and its associated mirror sites:

wuarchive.wustl.edu (US)

ftp.switch.ch (Switzerland)

ftp.funet.fi (Finland)

src.doc.ic.ac (UK)

archie.au (Australia)

McAfee provides technical support and product updates through America Online. The keyword for accessing the McAfee area is **MCAFEE**. If you have questions, please send e-mail to **MCAFEE**.

To Save system information using Device Manager

1. Click here  to start Device Manager.
2. Click Print button to print or save information to a file.

temp

Click here to receive information about the infected file.

Displays the name of the file being infected.

Displays the status of the infected file.

Initiates scanning for viruses.

Terminates scanning for viruses.

Resets all options to defaults. If you click this button, previous scan options will be cleared.

Displays where Scan will begin scanning for viruses. To specify a different location, choose Browse.

Click here to specify where you want Scan to begin its search for viruses.

Selecting this option instructs Scan to search for viruses in all the subfolders within your main folder.

Selecting this option instructs Scan to search for viruses inside every file it finds.

Selecting this option instructs Scan to only search for viruses inside program files.

Selecting this option instructs Scan to search for viruses inside files compressed with PkLite and LZEXE.

Click here to specify program file extensions.

Use this field to specify the action to be taken when a virus is found.

Selecting this option instructs Scan to display a custom message upon virus detection. For the message to be displayed, the Action option must be set to Prompt for action.

Enter the desired message to be displayed upon virus detection.

Selecting this option instructs Scan to sound an alert upon virus detection. Alert sounds at end of scan.

Selecting this option instructs Scan to log the names of the infected files.

Enter the desired log file in the provided text box.

Selecting this option instructs Scan to create and maintain a log file no larger than the size specified. Deselect this option for unlimited log file size.

Enter the desired size in the provided spin box.

Displays program file extensions.

Click here to add another program file extension.

Click here to delete the selected extension.

Click here to use Scan default program file extensions.

Click here to clean the virus from the file.

Enter new program file extension here.

Click here to delete infected file.

Click here to move the infected file to another directory.

Displays the filename in MS-DOS format.

Displays the infected file name.

Displays the infected file type.

Displays the virus name(s).

Displays the virus name(s).

Click here to continue scanning.

Displays the infected file size.

Click here to abort scanning.

Displays the size of the virus.

Displays the file location.

Displays what kind of objects the specified virus usually infects.

Displays the date that the file was created.

Indicates the date that the information in this file was last changed.

Indicates the date that this file was last opened.

Indicates whether the selected file is read-only; meaning it cannot be changed or accidentally deleted.

Indicates whether the selected file is hidden; meaning that you cannot see or use it unless you know its name.

Indicates whether the selected file should be archived. Some programs use this option to control which files are backed up.

Indicates whether the selected virus is polymorphic.

Indicates whether the selected file is a system file. System files are required by Windows in order to run properly, and by default are not shown in folder listings. Do not delete system files.

Indicates whether the selected virus can be removed.

Indicates whether the selected virus is memory resident.

Indicates whether the selected virus is encrypted.

Click here to select file to be used for logging.