WScanNT Help - Contents

WScanNT Help - Reference

About WScanNT

McAfee's WScanNT program detects, identifies, and disinfects known DOS computer viruses. WScanNT checks memory and both the system and data areas of disks for virus infections. If WScanNT finds a known virus, in most cases it will eliminate the virus and fully restore infected programs or system areas to normal operation. To obtain a list of viruses that WScanNT detects, choose Scan|Virus List or click the Virus List icon.

In addition, WScanNT can also assign validation and recovery codes to files, and use those codes to detect and treat infection by new and unknown viruses. If WScanNT has stored validation or recovery data for files, it may detect file changes and warn that infection by an unknown virus may have occurred. WScanNT can also use the recovery information to remove new or unknown viruses and restore infected files, master boot records (MBRs), and boot sectors.

WScanNT is designed to check for pre-existing infections of known and unknown viruses on floppy, hard, CD-ROM, and compressed (SuperStor, Stacker, DoubleSpace, and so on) disks on both stand-alone and networked personal computers, as well as network file servers. If you have a Novell NetWare/386 V3.11 or 4.0 file server, you may want to use the NetShield virus prevention software NetWare Loadable Module in conjunction with WScanNT.

Starting WScanNT

To start WScanNT

In the Program Manager, double-click the **WScanNT** icon.

The WScanNT main window appears.

As it loads, WScanNT performs a self-check of its program files to verify their integrity. It displays the scanning messages in the Report Summary area and displays any messages in the Messages area of the main WScanNT window.

WScanNT does not check diskettes or fixed disks at startup. To scan disks, see Scanning your system.

See also

If you find a virus
Cleaning your system

Configuring WScanNT using the WScanNT Notebook

Tasks

Displaying the WScanNT Notebook
Moving to the next Notebook page
Moving to a previous Notebook page
Closing the Notebook

Notebook Pages

Click	To change	Click	To change
	Control settings		Validation settings
	Action settings		Validation exceptions
	Report settings		

See also

Selecting items to scan
Scanning your system
Cleaning your system

Scanning your system

Background

- About scanning
- When to scan

Before you scan

- Selecting items to scan
- Configuring WScanNT
- Using settings files

Scanning

- Using profiles
- Scanning your system

After you scan

- If you find a virus
- Using the main WScanNT window
- Troubleshooting
- Cleaning your system
- Using the activity log

If you find a virus

DO NOT RUN ANY OTHER PROGRAMS - especially if the virus is found in memory. For more information, see Virus in memory.

If WScanNT finds one or more viruses, you will see a message in the main WScanNT window. Do not panic, even if the virus has infected many files.

If a virus is resident in memory, DO NOT use WScanNT to remove it because Windows or other system files might be infected and you risk spreading the virus. If you have detected such a virus, restart your computer and run the command line Scan program from your clean startup diskette.

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

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.

See also

Backing up your hard disk
Cleaning your system
Troubleshooting
False alarms

Cleaning your system

Clean your system when you know or suspect that a virus infection has occurred. If a virus is resident in memory, the most secure way to clean your system is to turn off your computer and start from a clean start-up diskette. However, you can securely use WScanNT to clean infections if:

- You are *absolutely sure* your system is virus-free (no viruses are resident in memory), AND
- You are *absolutely sure* that no system or WScanNT files are infected and spreading the infection when running.

Background

- About cleaning
- When to clean

Before you clean

- Selecting drives to clean
- Configuring WScanNT
- Using settings files

Cleaning

- How to clean your system
- Using profiles

After you clean

- Using the main WScanNT window
- Using the activity log
- Troubleshooting
- If a virus cannot be removed

Troubleshooting

Preventing viruses

Although McAfee VirusScan is designed to give 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 about 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 Bulletin Board Systems (BBSs), check with the SysOp about their scanning procedures. Many SysOps scan for viruses before making files available for download.

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

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.

See also

Obtaining new versions
Developing a security program
Making regular backups

Tips

Upgrading McAfee software

Unfortunately, new viruses (and variants of old ones) appear and circulate often in the personal computer community. Fortunately, McAfee usually updates the VirusScan programs monthly, and more often if many new viruses appear. Each new version may detect and eradicate as many as 60 to 100 new viruses, and may include new features. To find out what is new, review the on-line documentation files.

See also

Contacting McAfee
Obtaining new versions
Validating WScanNT programs
Updating your clean startup diskette

Contacting McAfee

Choose **Help|Product Support** to find out more information about McAfee technical support.

About McAfee

Before you contact 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
Overseas	Authorized Agents (overseas only)

List of installed files

WScanNT Files	Description
CLEAN.DAT	Virus removal data file required by WSCANNT.EXE.
FILE_ID.DIZ	Description of VirusScan used by some BBS software.
NAMES.DAT	Virus name data file required by WSCANNT.EXE.
PACKING.LST	List of all files, including validation information.
PROFILE1.PRF	Sample profile for scanning the C: drive.
PROFILE2.PRF	Sample profile for scanning the A: and B: drives.
README.1ST	Late-breaking information and new instructions not contained in this manual.
SCAN.DAT	Virus string data file required by WSCANNT.EXE.
VALIDATE.EXE	Used to check VirusScan programs for authenticity.
WSCANNT.EXE	The WScanNT program.
WSCANNT.HLP	WScanNT online help.
WSCANNT.INI	WScanNT initilization file.

Scan (DOS) Files	Description
SCAN.EXE	The Scan command line program.

Scan command line options

Click the command for its WScanNT equivalent, if applicable.

Option	Description
/? or /HELP	Display help screen.
/ADL	Scan all local drives (except floppy drives).
/ADN	Scan all network drives.
/AF {filename}	Store validation/recovery codes in filename.
/ALERT {servername}	Alert the servername server about infected files.
/ALL	Scan all files, not just standard executables.
/APPEND	Append to, rather than overwrite, the file (/REPORT).
/AV	Add validation/recovery data to program files.
/BOOT	Scan boot sector and master boot record only.
/CF {filename}	Check validation/recovery codes in filename.
/CLEAN	Clean up infections in boot sector, master boot record, and files when possible.
/CV	Check validation/recovery data in files.
/DEL	Overwrite and delete infected files.
/EXCLUDE {filename}	Exclude from scan any files listed in filename (with /AV).
/FAST	Speed up VirusScans scanning; may detect fewer

	viruses.
/LISTEN {servername}	Load Scan and wait for a command from the servername server.
/LOAD {filename}	Use Scan settings stored in filename.
/LOG	Save date and time VirusScan was last run in WSCANNT.LOG.
/MANY	Scan multiple floppies.
/MOVE {directory}	Move infected files to directory.
/NOCOMP	Skip checking of compressed executable files created with the LZEXE or PKLITE compression programs.
/NOBREAK	Disable Ctrl-C and Ctrl-Brk during scan.
/NOMEM	Skip memory checking.
/PAUSE	Enable screen pause.
/PLAD	Preserve last access dates on Novell drives.
/REPORT {filename}	Create report of infected files found during scan in filename.
/RF {filename}	Remove validation/recovery codes in filename.
/RPTCOR	Add list of corrupted files to the report file (/REPORT).
/RPTERR	Add list of system errors to the report file (/REPORT).
/RPTMOD	Add list of modified files to the report file (/REPORT).
/RV	Remove validation/recovery data from files.
/SHOWLOG	Display information in WSCANNT.LOG.
/SUB	Scan subdirectories inside a directory.
/VIRLIST	Display list of viruses detected by VirusScan.

Error codes

After WScanNT has finished running, it sets the ERRORLEVEL. You can use the ERRORLEVEL in batch files to take different actions based on the results of the scan.

WScanNT returns the following ERRORLEVELs:

Error	Description
0	No error occurred and no viruses were found.
1	An error occurred while accessing a file (reading or writing).
2	A VirusScan database (*.DAT) 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 an operation.
6	An internal program error occurred.
7	An error occurred in accessing in 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 command line.
10	A virus was found in memory.
11	An internal program error occurred.
12	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 was found in the master boot record, boot sector, or file(s).
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; WScanNT adds 100 to original error number.

About McAfee

Founded in 1989, McAfee Inc., is the leading provider of tools for productive computing for the 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 worlds 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 more than 50 countries worldwide.

Before you contact McAfee

Have the following information ready:

- Program name and version number.
- Type and brand of computer, hard disk, and any peripherals.
- Version of Windows NT, along with any device drivers in use.
- 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.

See also

Contacting McAfee
Troubleshooting
Error codes

Using the main WScanNT window

The main WScanNT window is the window that appears when you first start WScanNT.

Using the toolbar

Whenever WScanNT scans system memory, diskettes, or hard disks, WScanNT reports the following information:

- Files that are possibly infected.
- Possibly Infected By the name of the virus infecting the associated file.
- Report of the scan results.
- Messages that provide status, warning, and error information encountered during the scan.

WScanNT performs a self-check when it loads to ensure the integrity of the WScanNT program and data files. If an error occurs, see Program fails on self-check.

See also

Clearing log messages
Scanning your system
Cleaning your system
If you find a virus
Troubleshooting

Selecting items to scan / clean

Before scanning or cleaning, you must select drives, directories, or files to scan. You can scan local drives, including diskette drives, as well as network drives. You can select up to 40 items to scan. By default, drive C is selected automatically.

To select drives, choose **File|Select Items to Scan** or click the **Select** icon. The Select Items to Scan dialog box appears.

- Using the Selections list
- Adding a drive
- Adding a directory
- Adding a file
- Removing an item
- Closing the dialog box

See also

- Scanning your system
- Cleaning your system
- Configuring WScanNT

Displaying the WScanNT Notebook

You can fine-tune the way WScanNT scans your system to increase system security, reduce scanning time, and perform specific tasks. For example, you can delete infected files automatically or move them to a quarantine directory, generate a report of scan results, use CRC integrity checking to detect unknown viruses, and so on. You select these options in the WScanNT Notebook, which contains several pages of scan options.

To display the WScanNT Notebook, click the Settings icon or choose any option from the Settings menu.

Selecting Control options

To change control settings, choose **Settings|Controls** or click the **Configure** icon to display the Controls page of the WScanNT Notebook. Choose any of these options.

Option	Description
Executables Only	Scan executable files only (COM, EXE, SYS, BIN, OVL, DLL).
Subdirectories	Scan subdirectories inside selected directories.
Compressed Executables	Scan compressed executable files created by the LZEXE or PKLITE utilities.
Turbo Mode	Speed up scanning; may detect fewer viruses.
Performance Packages	Select settings (see below).
Default	Select default control settings automatically.
Turbo	Select turbo control settings automatically.
Maximum	Select maximum control settings automatically.

See also

Configuring WScanNT

Selecting Action options

To change action settings, choose **Settings|Actions** or click the **Action** tab to display the Actions page of the WScanNT Notebook. Choose any of these options.

Option	Description
Clean Infection (File, Boot Sector, MBR)	Clean up infections in boot sector and files when possible.
Delete Infected File	Overwrite and delete infected files.
Move Infected File to Directory	Move infected files to a quarantine directory.
Browse	Select a quarantine directory.

See also

- Cleaning your system
- Configuring WScanNT

Selecting Report options

About reports

To change report settings, choose **Settings|Reports** or click the Reports tab to display the Reports page of the WScanNT Notebook. Choose any of these options.

Option	Description
Report File Name	Type a report file name.
Browse	Select a report file from a list.
Append to Report File	Append report information to an existing report file.
Include Corrupted Files	Include corrupted files in the report.
Include Modified Files	Include validated files that have been modified in the report.
Include System Errors	Include system errors in the report.
Maintain Activity Log	Keep track of scan activities in a log file.
Keep Last 10 Events	Limit the number of saved scans to 10.

See also

Configuring WScanNT

Printing reports

Selecting Validation options

To change validation settings, choose **Settings|Validations** or click the Validations tab to display the Validations page of the WScanNT Notebook. Choose any of these options.

Option	Description
Use Codes Appended to Files	Store recovery/validation codes in validated program files.
Use Codes in External File	Store recovery/validation codes in an external validation database file.
Database File	Specify a validation database file.
Browse	Select a validation database file from a list.
Add Codes	Add validation codes.
Check Codes	Check existing validation codes.
Remove Codes	Remove existing validation codes.

Note If you install new software on your system, you will need to update validation codes to include these new files. The fastest way to do this is to first select Remove Codes and scan your system, then select Add Codes and scan your system again.

See also

- Cleaning your system
- Configuring WScanNT
- Using validation / recovery codes

Changing the Exception List

If you set up validation codes on the Exceptions page of the WScanNT Notebook, subsequent scans can detect changes in validated files. This can generate false alarms if the executable files are self-modifying or self-checking (most programs that do this will tell you to turn off your anti-virus software before running them). Therefore, when using validation codes, specify an exception list to identify such files and exclude them from the validation. The exception list is an ASCII or DOS text file.

Command line equivalent is /EXCLUDE {*filename*}.

To change the exception list, choose **Settings|Exceptions** or click the **Exceptions** tab to display the Exceptions page of the WScanNT Notebook. Choose any of these options.

Option	**Description**
Exceptions File	Type a validation exceptions file name.
Browse	Select a validation exceptions file.
Save	Save changes to the list of files to exclude.
Files to Exclude from Validation	Display or change the list of files to exclude from validation.
Add	Add a file to the list of files to exclude.

See also

Using validation / recovery codes
Configuring WScanNT

Setting the scan schedule

You can schedule future times for WScanNT to scan your system automatically.

To change schedule settings, choose **Scan|Schedule** or click the **Schedule** icon to set or change prescheduled scans. Choose any of these options.

Option	Description
Active Schedules	Display a list of scheduled scans.
Add	Add a scheduled scan to the Schedule list.
Delete	Remove a scheduled scan from the Schedule list.
Close	Close the Scheduler dialog box.
Frequency	Set the scheduled scanning frequency.
Date	Set the scheduled day of the week or month.
Time of Day	Set the scheduled time of day.
All Local Drives	Scan all local drives.
All Network Drives	Scan all network drives.
Select	Select drives, directories, and for the scheduled scan.
Options	Select scanning options in the WScanNT Notebook for the scheduled scan.

See also

About Scheduling
Configuring WScanNT

About scanning

WScanNT can detect known, new, and unknown viruses.

Known virus detection

WScanNT detects known viruses by searching the system for known characteristics (sequences of code) unique to each computer virus and reporting their presence if found. For viruses that encrypt or cipher their code so that every infection is different, WScanNT uses detection algorithms that work by statistical analysis, heuristics, and code disassembly.

New and unknown virus detection

WScanNT can also check for new or unknown viruses by comparing files against previously recorded validation data. If a file has been modified, it will no longer match the validation data, and WScanNT will report that the file may have become infected. With certain options, cleaning can restore infected files, master boot records (MBRs), or boot sectors.

When to scan

It is wise to scan your disks when you introduce new programs or disks that may be infected.

Scan your system when you:

- Insert an unchecked diskette
- Install or download new files

Scanning steps

Scan your system when you want to detect and identify viruses.

To scan

1 Select the scan settings you want.

2 Select the items you want to scan. You must select at least one item to scan (by default, drive C is selected). WScanNT saves the items in the WSCANNT.INI file.

Alternatively, you can drag selected files or directories from Windows File Manager and drop the selected items onto the main WScanNT window. WScanNT does not save the names of the files or directories to the WSCANNT.INI file.

3 Choose the Scan icon or choose **Start Scan** from the Scan menu.

WScanNT performs the check according to the settings you have selected. You will see the names of files being scanned in the status bar, and you will see any status or warning messages in the main WScanNT window.

See also

If you find a virus

About cleaning

Basic principles to minimize damage

- Before cleaning your system, back up all of your programs and data.

  Of course, this works best if you back up regularly, so that you can restore from a backup made before your system was infected. But even a backup from an infected system can be useful for restoring data because most viruses do not corrupt data. If a program no longer runs after being cleaned, replace it from the original disk or from a virus-free backup.
- When disinfecting an infected system, it is important to start from a sterile field.
- Restart your computer from a clean, write-protected diskette.

Background

Although cleaning removes many viruses and restores normal operation, viruses can be harmful and insidious, and no anti-virus program can undo all their damage. Between 10% and 20% of all viruses actually corrupt the files they infect. If the file is infected with an uncommon virus that WScanNT cannot restore, WScanNT notifies you and identifies the filename. Write down this filename so that you can restore it from a backup diskette or tape.

If you use both the **Clean Infection (File, Boot Sector, MBR)** and the **Delete Infected File** options, WScanNT will first attempt to disinfect an infected file and, if the file is damaged beyond repair, delete the infected file. Deleted files are not recoverable except from backups.

Some viruses damage or overwrite program files or overlay files. Removing the virus can truncate the file or otherwise render it inoperable. Others, like the common virus Stoned, infect the master boot record (MBR). On systems partitioned with programs other than DOS (such as Disk Manager and SpeedStor), removing the virus can cause loss of the master boot record (MBR) and all data on the disk.

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.

Note To use WScanNT to clean up infected files, the CLEAN.DAT file *must* be present in the WScanNT subdirectory. If you do not have the CLEAN.DAT file, first verify whether you should contact your system administrator or information systems staff directly for virus clean-up. Otherwise, you can contact McAfee.

When to clean

Clean when you find or suspect a virus infection in your system.

How to clean your system

To clean

1 Select the items you want to clean. You must select at least one item to scan (by default, drive C is selected).

2 Select the clean settings you want.

3 Select Clean Infection (File, Boot Sector, MBR) on the Actions page of the WScanNT Notebook.

4 Click the Scan icon, or choose **Scan|Start Scan**.

WScanNT performs the check according to the settings you have selected. You will see the names of files being scanned in the status bar, and you will see any status or warning messages in the main WScanNT window.

WScanNT reports the results of its attempt to remove the virus from each infected file. If a file has several infections, it will report on each.

If viruses were safely removed, rescan and check diskettes. If WScanNT has successfully removed all the viruses, turn your computer off again and restart from the system disk. Scan your hard disks again to make sure they are virus-free. If you suspect that your system was infected from a diskette, run WScanNT from your hard disk to examine and disinfect the diskettes you use.

See also

If a virus cannot be removed

If a virus cannot be removed

If WScanNT cannot remove a virus, a message appears:

```
Virus cannot be safely removed from this file.
```

Write down the filename or generate a report so that you know what to restore from backups.

See also

Cleaning
Contacting McAfee

Selecting control options automatically

Choose one of these buttons to selects the following controls options automatically.

Option	Default	Turbo	Maximum
Executables Only	X	X	
Subdirectories		X	X
Compressed Executables	X		X
Turbo Mode		X	

See also

Selecting Configuration options

Using validation / recovery codes

Background

- About validation / recovery codes

Ways to validate

- Preferred - storing codes in a single file
- Optional - storing codes in validated files

Bypassing self-checking or self-modifying files

- Excluding files from validation

Managing validation codes

- Adding validation
- Checking validation
- Removing validation

See also

- Selecting Action options

About validation / recovery codes

If your environment is highly vulnerable to viruses, or you require unusual security against them, you can use WScans validation and recovery options. WScanNT checks for new or unknown viruses by comparing files against previously recorded validation data. If a file has been modified, it no longer matches the validation data, and WScanNT reports that the file may have become infected.

WScanNT has two levels of validation, which are stored in two separate ways:

- Storing codes in a single Use Codes in External File. WScanNT can store the enhanced code in a separate recovery file, which can be stored off-line (for example, on a diskette) for recovery purposes. This is the preferred method because it stores the data for files, the boot sector, and the master boot record (MBR) of a disk in the recovery file.
- Storing codes in validated files. WScanNT can append a simple 98-byte validation code to .COM and .EXE files. This method applies only to the files you specified. It does not store data for the boot sector and master boot record (MBR).

Once the validation / recovery codes are stored, WScanNT can check them to detect changes to the files. More importantly, if you have stored the recovery information with /AF, WScanNT can use it to restore infected files, master boot records (MBRs), and boot sectors.

All of these options require continuing effort to store and maintain the codes. For example, if you install new programs or upgrade old ones, you should use the Remove option to remove all the codes, then the Add option to restore them.

If you install new software, or upgrade your DOS version, remember to update your recovery file.

See also

Using validation / recovery codes

Storing codes in an external data file

Storing codes in a single file is PREFERRED to Storing codes in all files because

- You can store the recovery file off-line (on your clean anti-viral startup diskette, for example, or on a network drive or tape drive). You can also access it on demand to check for, and recover from, infection by unknown viruses.
- It keeps self-checking files (usually copy-protected programs) from reporting that they have been tampered with.
- You do not need an exception list. However, it is important that you run WScanNT with the /RF option on individual self-modifying files, such as Lotus 1-2-3, to remove the validation codes for those programs from the validation file.

Command line equivalents are /AF, /CF, and /RF.

See also

Using validation / recovery codes

About validation / recovery codes

Storing codes in validated files

Storing codes in all files is useful primarily for companies that distribute software to their customers or employees, and want to incorporate an additional level of virus protection.

The preferred method is storing codes in a single file.

Command line equivalents are /AV, /CV, and /RV.

See also

- Using validation / recovery codes
- About validation / recovery codes

About reports

You can create a report that describes the results of your scan. A report includes information about the items scanned, infections found, infections cleaned, and optional details about corrupted files, modified files, and system errors.

See also

Selecting Report Options

About scheduling

You can schedule WScanNT to automatically scan at a future date and time. Thereafter, WScanNT runs the scan at the scheduled time *if* the workstation is running and WScanNT is loaded, even if you are using another application at the time.

In this way, you can scan your system unattended and ensure that scanning occurs on a regular basis. For each scheduled scan, you can specify when to scan, what to scan, and which scan options to use. WScanNT saves the information for each scheduled scan in a separate .VSS file.

See also

Selecting Scheduling Options

Interacting with your network

Many personal computers are interconnected through a local area network (LAN). WScanNT is highly compatible with most networks. Here are some ways of using the WScanNT software with your network:

Run WScanNT on network drives

When WScanNT runs from a workstation (PC) on the network, it checks network drives for viruses just as it does local drives. For convenience, if the Network Drives check box on the Scheduler dialog box is selected, WScanNT scans all network drives to which the workstation is connected.

Use NetShield

McAfee's NetShield program provides continuous virus protection on a NetWare server. NetWare network administrators can use it to check for both known and unknown viruses and to monitor all network activities.

Developing a security program

See also

Tips

Developing a security program

WScanNT has been shown to be an effective virus-prevention tool that can be of significant value when used in a conscientiously applied program of network hygiene.

WScanNT is only one important element. A comprehensive computing security program includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and administrator awareness. Even with WScanNT, some viruses--along with theft or fire--can render a disk unrecoverable without a recent backup.

If you are a network administrator, we urge you to implement a security program to safeguard your organizations data and productivity. If you are a network user, please support and comply with such a program.

See also

Tips

Backing up your system

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

To increase your chance of recovery, copy all the files on all of your hard disks onto clean diskettes or a backup tape. You can use a commercial backup program, or the one included with DOS or OS/2. Scan the program disk first to make sure 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 not. However, do not overwrite previous backup disks or tapes, which may not be infected.

See also

Tips

General abnormalities

Using WScanNT with other anti-virus software

When you run more than one anti-virus program, you risk strange results and false alarms. For example, some anti-virus programs store their virus signature strings unprotected in memory. Running a WScanNT program may detect them.

See also

Troubleshooting

False alarms

Due to the nature of anti-virus software, there is a possibility that WScanNT may report a virus in a file that is not infected. This can be more likely if you are using more than one brand of virus protection software, especially if the virus is reported in memory. WScanNT may also incorrectly report a virus in the boot sector or master boot record of certain copy-protected diskettes.

If WScanNT reports a virus infection that you suspect may be in error, contact McAfee.

You can upload the file to our BBS.

See also

Troubleshooting

Virus in memory

If you find a virus in memory, TURN OFF YOUR MACHINE, then run the Scan command line program from a clean start-up diskette. DO NOT use WScanNT to remove a virus that is resident in memory.

See also

Troubleshooting

Program fails on self-check

WScanNT performs a self-check when run. If WScanNT has been changed in any way, a warning appears in the Message window and WScanNT exits and returns you to the Windows Program Manager. We recommend that you quit, then run the command line Scan program from a clean start-up diskette before continuing.

See also

Troubleshooting

Obtaining new software versions

As a WScanNT licensee, you may download new versions from the McAfee BBS without charge for one year from your date of purchase.

You may also use your own communications software to download new versions from the McAfee bulletin board, CompuServe, America Online, or the Internet. See Chapter 1, Welcome to VirusScan, and Appendix A, Retrieving McAfee programs with communications software, in the *Using VirusScan* documentation, for more information.

New versions of McAfee software are stored in compressed form to reduce transmission time. You can download the PKUNZIP utility to decompress files yourself.

Always download and decompress the files in a separate directory from your current files. That way, if you discover a problem with the new files, you will still have the old ones.

See also

Upgrading

Validating McAfee software

If your new copy of WScanNT differs from the validation data, it may have been damaged. Do not use it, and obtain a clean copy of WScanNT from a known source.

When you download a program file from any source other than the McAfee BBS or other McAfee service, it is important to verify that it is authentic, unaltered, and uninfected. McAfee anti-virus software includes a program called Validate that helps you do this. When you receive a new version of WScanNT, run Validate on all of the program files.

To do this for WScanNT, start from the system prompt (C> or C:\).

1 Navigate to the directory to which you have downloaded the files. For example, if you have stored the files in C:\MCAFEE\DOWNLOAD\VIRUSCAN:

```
C> c:
C> cd \mcafee\download\viruscan
```

2 Type the following command

```
DOS or Windows      C> validate SCAN.EXE
```

3 Compare the results with the information in the PACKING.LST file or on-line documentation file for the program you validated. If the validation results match what is in the file, it is highly unlikely that the program has been modified.

See also

Upgrading

Updating your clean startup diskette

Once you have validated the new version, copy it into your C:\MCAFEE directory. In addition, copy the WScanNT program onto your clean startup diskette. Here is a way to do this from the command prompt.

Note any changes you have made to default options because you may want to select and save them again. Start from the system prompt (C> or C:\).

1 Navigate to the directory to which you have retrieved the files, such as C:\MCAFEE\DOWNLOAD\VIRUSCAN:

```
C> c:
C> cd \mcafee\download\viruscan
```

2 Copy the contents of the directory to C:\MCAFEE

```
C> copy *.* c:\mcafee
```

3 Temporarily remove write-protection from your clean start-up diskette and insert it in drive A.

For a 3.5" diskette, slide its corner tab so that the square hole is *closed*.

For a 5.25" diskette, remove the tab from its corner notch.

4 Copy the WScanNT program to the diskette.

```
DOS or Windows      C> copy SCAN.EXE a:
```

5 Remove the diskette from the drive and ***write-protect it*** again.

See also

Upgrading

About the WScanNT Notebook

The WScanNT Notebook contains pages of WScanNT options. Before you scan, select the options you want.

See also

Configuring WScanNT
Displaying the WScanNT Notebook

Inserting an unchecked diskette

Scan whenever you insert an unchecked diskette in a diskette drive.

Every time you insert a new diskette in your drive, run WScanNT on it before executing, installing, or copying its files. In fact, we recommend doing this now with all the diskettes you normally use.

See also

When to scan

Installing or downloading new files

Every time you install new software on your hard drive, or download executable files from a network server, bulletin board, or on-line service, run WScanNT on that drive BEFORE executing the files.

If you install any new software or programs on your system and are running WScanNT with the validation options, you need to add validation codes to the new files. The quickest way to update the validation codes is to remove all validation codes from the hard disk and then add them back.

See also

When to scan

Using validation codes

Using profiles

A *profile* is a simplified way to scan your system using scan options stored in a profile load file. Using profiles automates repetitive scanning tasks and makes it easier to scan your system

Before using profiles, they must be defined in the WSCANNT.INI file. If no profiles are available, you (or your system administrator or information systems staff) must create them, then reload WScanNT. For instructions, see Setting up profiles.

See also

Selecting a profile
Setting up profiles
Formatting a profile file

Setting up profiles

Before you can select profiles from the Run Profile dialog box, the profiles must be defined in the WSCANNT.INI file. Once defined, you must restart WScanNT for your changes to take effect.

Contact your system administrator or information services staff before attempting this procedure yourself. They might want to perform this procedure for you.

To set up or modify a profile, you need to use a text editor that can read and save WSCANNT.INI as an ASCII text file. You also need to create the scan load file you want to use for each profile, as described in the discussion of the /LOAD option in Chapter 4 of the VirusScan *User's Guide*.

Heres an example of the settings for the header variables in the WSCANNT.INI file.

```
Header1=Profile Engine v1.0
Header2=Select a profile to run, please
```

Heres an example of the settings for one of the buttons in the WSCANNT.INI file.

```
[Profile1]
Label=Hard Disk
Description=Scan disk C:
File=c:\mcafee\profile1.prf
```

- `[Profile1]` begins the section for the first button (the next button is *Profile2*, and so on).
- `Label` is the short word or phrase that appears in the button.
- `Description` is the text that provides additional information about the profile and appears to the right of the button.
- `File` identifies the name and path of the profile file. If WScanNT cannot locate the specified file, the button is dimmed (unavailable).

You can specify these settings for up to four profiles.

See also

Using profiles
Selecting a profile
Formatting a profile file

Formatting a profile file

A setting file is an ASCII text file. Use a text editor to create the file. You can put all Scan command line options on the same command line or put each option (with its parameter) on its own line, separated by a hard carriage return and line feed, as shown in the following examples.

Sample load file with all options on the same command line:

```
m: /report a:infectn.rpt /rptcor /rpterr
```

Sample profile file with each option on a separate command line:

```
m:
/report a:infectn.rpt
/rptcor
/rpterr
```

See also

- Using profiles
- Selecting a profile
- Setting up profiles

Using settings files

You can save the scan settings and the selected items in a settings (.INI) file. That way, you don't need to select scanning options and items individually every time you want to scan--you simply load the settings file.

You can save default scan settings in WSCANNT.INI (WScanNT reads this file and uses these settings when it loads), or you can save them in a file with a different name.

Selecting a profile overrides the current scan settings you've loaded for the duration of the profile scan.

See also

Saving scan settings
Loading scan settings

Using the activity log

The *activity log* keeps track of the dates and times you scan your system, as well as associated messages regarding the items scanned and infections found. It provides an audit trail that you can use to verify regular scanning or, if you encounter an infection, to determine the last time the system was scanned for viruses and which items were found to be infected.

To update the activity log with each scan, the Maintain Activity Log check box must be selected on the Reports page of the WScanNT Notebook.

To view the activity log, choose Scan|Activity Log or click the Activity Log icon. The Activity Log dialog box appears.

See also

- Maintaining an activity log
- Setting the number of events stored in the activity log
- Specifying a different log file name
- Viewing the activity log
- Viewing activity log details
- Printing the activity log

Specifying a different log file name

The default file name for the activity log is WSCANNT.LOG. To specify a different log file name or path, use an ASCII text editor to change the **LogFile** variable in the **[Activity Log]** section of the WSCANNT.INI file, as shown in the following example.

```
[Activity Log]
LogFile=c:\mcafee\logfile\myscan.log
```

Using the Toolbar

The toolbar on the main WScanNT window contains icons that you can click with a mouse.

See also

- Profiles
- Scan
- Select
- Settings
- Virus List
- Schedule
- Activity Log

Contents of the WSCANNT.INI file

Section name	Variable Name	Default Setting
[Profiles]	Header1	Select a profile to run or edit the file
	Header2	WSCANNT.INI to change or add profiles.
[Profile1]	Label	Hard Disk
	Description	Scan standard files on disk C:
	File	profile1.prf
[Profile2]	Label	Floppy disks
	Description	Scan disks A and B
	File	profile2.prf
[Profile3]	Label	Unavailable
	Description	
	File	
[Profile4]	Label	Unavailable
	Description	
	File	
[Main]	PS_O_LOCAL	0
	PS_O_NETWORK	0
	PS_O_EXTERN	0
	PS_O_REPORT	0
	PS_O_DATABASE	0
	PS_O_OPTIONS	0
	PS_O_PRIVATE	0
	PS_O_RINF	0
	PS_O_RERS	0
	PS_O_RPRG	0
	PS_O_NADM	0
	PS_O_ANALYZER	0
	PS_O_APPEND	0
	PS_O_ARC	0
	PS_O_BINARY	0
	PS_O_CMPFIL	1
	PS_O_CORRUPT	0
	PS_O_DELCOR	0
	PS_O_DELINF	0
	PS_O_DELUNF	0
	PS_O_DFC	0

	PS_O_ERRORS	0
	PS_O_MOD	0
	PS_O_MOVCOR	0
	PS_O_MOVINF	0
	PS_O_NOTIFY	0
	PS_O_PROMPT	0
	PS_O_REMOVE	0
	PS_O_SMLBFR	0
	PS_O_STDEXT	1
	PS_O_SUBDIR	0
	PS_O_TRACER	0
	PS_O_VAL	0
	PS_O_ERRDISKFORMAT	0
	PS_O_ERRMEDIA	0
	PS_O_ERRFILESYSTEM	0
	PS_O_ERRNETWORK	0
	PS_O_ERRFILEACCESS	0
	PS_O_ERRDEVICEACCESS	0
	PS_O_ERRREPORTFAILURES	0
	PS_S_ADMIN	
	PS_S_CORRDIR	
	PS_S_CORRUPT	
	PS_S_ERRORS	
	PS_S_EXCEPT	
	PS_S_EXTEN	
	PS_S_INFDIR	
	PS_S_INFECT	
	PS_S_MODIF	
	PS_S_REPORT	
	PS_S_SERVER	
	PS_S_START	C:;;;
	PS_S_SUSPIC	
	PS_S_VALID	
[Activity Log]	KeepLog	1
	LogFile	wscannt.log

Last10	0

Displaying infected files

The **File** list on the main WScanNT window contains a list of files that may be infected. The Infection list contains the name of the virus that may have infected the file.

Displaying the virus causing the infection

The **Possibly Infected By** list on the main WScanNT window contains the name of a virus that may have infected the associated file in the File list.

Displaying report summary information

The **Report** summary area on the main WScanNT window contains a summary of the results of a scan.

It shows the number of files, boot sectors, and master boot records that were scanned, analyzed, and, if applicable, infected.

Clearing log messages

Choose the **Clear** button to clear log messages that appear in the Messages list.

A dialog box asks you to confirm that you want to clear messages. Choose **Yes** to clear them, or choose **No** to keep them.

Display scan output messages

The **Messages** list on the main WScanNT window displays messages describing what WScanNT found while scanning, including infections, corruptions, system errors, and a summary of results.

Moving to the next page in the WScanNT Notebook

Choose the **>>** (**Next**) button to move to the next page in the WScanNT Notebook.

This button is dimmed if you are on the last page in the Notebook.

Moving to the previous page in the WScanNT Notebook

Choose the **<<** (**Previous**) button to move to the previous page in the WScanNT Notebook.

This button is dimmed if you are on the first page in the Notebook.

Closing the WScanNT Notebook

Choose the **Close** button on any page to close the WScanNT Notebook and return to the main WScanNT window.

Scanning executable files only

Select the **Executables Only** check box on the Controls page of the WScanNT Notebook to scan files with standard extensions.

Executables Only reduces scan time by checking only files with standard extensions: .EXE, .COM, .SYS, .BIN, .OVL, or .DLL. If this option is not selected, WScanNT checks all files on the selected drives and directories, which increases scan time. Do not use this option if you have found a virus or suspect one.

Command line equivalent, if this option is not selected, is /ALL.

Scanning subdirectories

Select the **Subdirectories** check box on the Controls page of the WScanNT Notebook to scan subdirectories.

Subdirectories tells WScanNT to check files in the subdirectories of selected directories. If this option is not selected, WScanNT ignores subdirectories. You do not need to select this option if you are scanning an entire drive.

Command line equivalent is /SUB.

Scanning compressed executable files

Select the **Compressed Executables** check box on the Controls page of the WScanNT Notebook to scan compressed executable files.

Compressed Executables tells WScanNT to check inside executable, or self-decompressing, files that have been compressed using the LZEXE or PKLITE file compression programs. If selected, WScanNT decompresses each file in memory and checks for viruses signatures. If this option is not selected, WScanNT does not check *inside* compressed files for viruses, although it can check for modifications if the validation options are used.

Command line equivalent, if this option is not selected, is /NOCOMP.

Using the turbo mode

Select the **Turbo Mode** check box on the Controls page of the WScanNT Notebook to use WScanNT's Turbo mode.

Turbo reduces scan time by examining a smaller portion of each file. This takes less time but might miss some infections. Therefore, do not use this option if you have found a virus or suspect one.

Command line equivalent is /FAST.

Choosing default settings

Choose the **Default** button to select program default settings on the Controls page of the WScanNT Notebook.

Choosing this button overrides any settings you may have selected individually or by choosing other Performance Packages, such as the Optimal or Maximum buttons.

Choosing optimal settings

Choose the **Optimal** button to select optimal settings on the Controls page of the WScanNT Notebook.

Choosing this button overrides any settings you may have selected individually or by choosing other Performance Packages, such as the Default or Maximum buttons.

Choosing maximum settings

Choose the **Maximum** button to select the maximum settings on the Controls page of the WScanNT Notebook.

Choosing this button overrides any settings you may have selected individually or by choosing other Performance Packages, such as the Default or Optimal buttons.

Cleaning infected files

Select the **Clean Infection (File, Boot Sector, MBR)** check box on the Actions page of the WScanNT Notebook to clean virus infected files.

Cleaning tells WScanNT to attempt to restore the boot sector and any infected files. Between 10% and 20% of all viruses are not removable; they damage the infected file beyond repair. If the infected file resides on a network drive, you must have rights to change files on that drive. If WScanNT cannot restore a file, you will see a message that identifies the name of the unrecoverable file. If **Clean Infection (File, Boot Sector, MBR)** is not selected, WScanNT merely reports the infection in the main WScanNT window.

Note To select this option, the CLEAN.DAT file must reside in the WScanNT directory. If the file does not exist, contact your system administrator or information systems staff to determine whether they will clean your system instead. Otherwise, contact McAfee.

- We recommend selecting both **Clean Infection (File, Boot Sector, MBR)** and Delete Infected File so that WScanNT attempts to repair the infected file first, then deletes the file only if it cannot be recovered. In addition, **Clean Infection (File, Boot Sector, MBR)** can remove master boot record (MBR) and boot sector viruses, but **Delete Infected File** alone cannot.
- Alternatively, we recommend selecting both **Clean Infection (File, Boot Sector, MBR)** and Move Infected File to Directory so that WScanNT attempts to repair the infected file first, then moves it to the quarantine directory only if it cannot be recovered. In addition, **Clean Infection (File, Boot Sector, MBR)** can remove master boot record (MBR) and boot sector viruses, but **Move Infected File to Directory** alone cannot.

We also recommend that you get help to deal with a virus if you are unfamiliar with anti-virus software. This is especially true for "critical" viruses and master boot record / boot sector infections, because improper removal can result in lost data or damaged disks. See Contacting McAfee.

Command line equivalent is /CLEAN.

Deleting infected files

Select the **Delete Infected File** check box on the Actions page of the WScanNT Notebook to delete virus infected files.

Delete Infected File tells WScanNT to delete infected files automatically when found. Between 10% and 20% of all viruses are not removable; they damage the infected file beyond repair. Erased files cannot be recovered, so consider generating a report so that you know which files to restore from backups.

Note If the infected file resides on a network drive, you must be able to delete files on that drive.

We recommend selecting both **Delete Infected File** and Clean Infection (File, Boot Sector, MBR) so that WScanNT attempts to repair the infected file first, then deletes the file only if it cannot be recovered. In addition, **Clean Infection (File, Boot Sector, MBR)** can remove master boot record (MBR) and boot sector viruses, but **Delete Infected File** alone cannot.

We also recommend that you get help to deal with a virus if you are unfamiliar with anti-virus software. This is especially true for "critical" viruses and master boot record / boot sector infections, because improper removal can result in lost data or damaged disks. See Contacting McAfee.

Command line equivalent is /DEL.

Moving infected files to a quarantine directory

Select the **Move Infected File to Directory** check box on the Actions page of the WScanNT Notebook to move infected files to a quarantine directory.

If selected, you must type the path of the quarantine directory, or choose the Browse button to select one from a list.

We recommend selecting both **Move Infected File** and Clean Infection (File, Boot Sector, MBR) so that WScanNT attempts to restore the infected file first, then moves the file to the quarantine directory only if it cannot be recovered. In addition, **Clean Infection (File, Boot Sector, MBR)** can remove master boot record (MBR) and boot sector viruses, but **Move Infected File** alone cannot.

We also recommend that you get help to deal with a virus if you are unfamiliar with anti-virus software. This is especially true for "critical" viruses and master boot record / boot sector infections, because improper removal can result in lost data or damaged disks. See Contacting McAfee.

Command line equivalent is /MOVE.

Specifying the path of the quarantine directory

Type the path name of the quarantine directory (such as `c:\mcafee\quarntin`) in the text box, or choose Browse to select one.

Note To use this option, the Move Infected File to Directory check box must be selected.

Selecting a quarantine directory

Choose the **Browse** button on the Actions page of the WScanNT Notebook to select a quarantine directory from a directory list. The directory you select appears in the Quarantine Directory text box. Alternatively, you can type the path of the directory in the text box.

Note To use this option, the Move Infected File to Directory check box must be selected.

Selecting a quarantine directory in the Directory Selection dialog box

Use the Directory Selection dialog box to select a quarantine directory you want to use for infected files.

Select the Drive, if necessary, then select the Directory you want to use.

When finished, choose OK to close the dialog box and save the selection you've made, or choose Cancel to abandon your selection.

This dialog box appears when you choose Browse to select a Quarantine directory on the Actions page of the WScanNT Notebook.

Closing the Directory Selection dialog box

Choose **OK** on the Directory Selection dialog box to save the quarantine directory you've selected and close the dialog box.

Canceling and closing the Directory Selection dialog box

Choose **Cancel** on the Directory Selection dialog box to abandon the quarantine directory you've selected and close the dialog box.

Selecting a drive for the quarantine directory

Select a drive from the **Drives** list on the Directory Selection dialog box that contains the quarantine directory you want to use for infected files.

Selecting a quarantine directory

After you've selected a drive, select a directory from the **Directory** list on the Directory Selection dialog box for the quarantine directory you want to use for infected files.

Specifying the name of a report file

In the **Report File** Name text box on the Reports page, type the name and path of the report file you want to use or create (such as `c:\mcafee\myscan.rpt`) in this text box, or choose Browse to select one from a list of files.

Command line equivalent is /REPORT.

Selecting a report file

Choose the **Browse** button on the Reports page of the WScanNT Notebook to select a report file from a list of files. The file name you select appears in the Report File Name text box.

Command line equivalent is /REPORT.

Appending information to the report file

Select the **Append to Report File** check box on the Reports page of the WScanNT Notebook to add scan log information to the end of the specified report file.

Note If this check box is not selected, WScanNT overwrites the specified report file, if it exists.

Command line equivalent is /APPEND.

Including messages about corrupted files in the report file

Select the **Include Corrupted Files** check box on the Reports page of the WScanNT Notebook to include information about corrupted files in the specified report file.

If this check box is not selected, WScanNT excludes corruptions from the report file.

Command line equivalent is /RPTCOR.

Including warnings about modified files in the report file

Select the **Include Modified Files** check box on the Reports page of the WScanNT Notebook to include in the specified report file information about files that have been modified.

If this check box is not selected, WScanNT excludes warnings about modified files from the report file.

Command line equivalent is /RPTMOD.

Including system errors in the report file

Select the **Include System Errors** check box on the Reports page of the WScanNT Notebook to include information about system errors in the specified report file.

If this check box is not selected, WScanNT excludes errors from the report file.

Command line equivalent is /RPTERR.

Maintaining an activity log

Select the **Maintain Activity Log** check box on the Reports page of the WScanNT Notebook to keep information about each scan in a log file.

If selected, WScanNT saves the time and date at which a scan is run, as well as any results of the scan, by updating or creating an activity log file (by default, WSCANNT.LOG in the current directory).

If this check box is not selected, WScanNT does not maintain an activity log.

Command line equivalent is /LOG.

Setting the number of events stored in the activity log

Select the **Keep Last 10 Events** check box on the Reports page of the WScanNT Notebook to set to 10 the number of events stored in the activity log file.

The Maintain Activity Log check box must be selected for this option to have any effect.

Storing validation / recovery codes in program files

Select the **Use Codes Appended to Files** check box on the Validation page of the WScanNT Notebook to add, check, or remove validation / recovery codes in standard executable files, adding about 98 bytes to each file validated.

This method validates files but not the master boot record (MBR) or boot sector of a disk. If the executable files reside on a network disk, you must have sufficient rights to update them.

You must also select Add codes, Check codes, or Remove codes.

Note You can select either Use Codes Appended to Files or Use Codes in External File, but you cannot select both in the same scan.

See also

Using validation / recovery codes

Storing validation / recovery codes in an external file

Select the **Use Codes in External File** check box on the Validation page of the WScanNT Notebook to add, check, or remove validation / recovery codes in an external file you specify.

This method, which is the preferred method, validates files, the master boot record (MBR), and boot sector of a disk. If the database file resides on a network disk, you must have sufficient rights to create and delete it.

If selected, you must type the file name of the validation file, or choose Browse to select one from a list.

You must also select Add codes, Check codes, or Remove codes.

Note You can select either Use Codes Appended to Files or Use Codes in External File, but you cannot select both in the same scan.

See also

Using validation / recovery codes

Specifying the name of an external validation file

Type the name and path of the validation file you want to use or create (such as `c:\mcafee\valcodes.sav`) in this text box, or choose Browse to select one from a list of files.

Note To use this option, the Use Codes in External File check box must be selected.

See also

Using validation / recovery codes

Actions page

Selecting an external validation file

Choose the **Browse** button on the Validation page of the WScanNT Notebook to select a validation file from a list of files. The file you select appears in the Use Codes in External File text box.

Note To use this option, the Use Codes in External File check box must be selected.

See also

Using validation / recovery codes

Adding validation / recovery codes

Select the **Add Codes** radio button on the Validation page of the WScanNT Notebook to add validation / recovery codes to program files or to an external database file.

Note For this option to work, either the Use Codes Appended to Files or Use Codes in External File check boxes must be selected.

Command line equivalents are /AF for an external file and /AV for binary files.

See also

Using validation / recovery codes

Checking validation / recovery codes

Select the **Check Codes** radio button on the Validation page of the WScanNT Notebook to check validation / recovery codes that have previously been added in program files or in an external file.

Note For this option to work, either the Use Codes Appended to Files or Use Codes in External File check boxes must be selected.

Command line equivalents are /CF for an external file and /CV for binary files.

See also

Using validation / recovery codes

Removing validation / recovery codes

Select the **Remove Codes** radio button on the Validation page of the WScanNT Notebook to remove validation / recovery codes that have previously been added in program files or in an external file.

Note For this option to work, either the Use Codes Appended to Files or Use Codes in External File check boxes must be selected.

See also

Using validation / recovery codes

Adding a file to the validation exceptions list

Choose the **Add** button on the Exceptions page of the WScanNT Notebook to select a file to add to the current validation exceptions list.

See also

Using validation / recovery codes

Saving the validation exceptions list

Choose the **Save** button on the Exceptions page of the WScanNT Notebook to save the current validation exceptions list to the specified validation exceptions file.

Note This button is available only if you've changed the validation exceptions list.

See also

Using validation / recovery codes

Specifying the name of a validation exceptions file

Type the name and path of the validation exceptions file you want to use or create (such as `c:\mcafee\exceptn.vss`) in the **Exceptions File** text box, or choose Browse to select one from a list of files.

See also

Using validation / recovery codes

Exceptions page

Selecting a validation exceptions file

Choose the **Browse** button on the Exceptions page of the WScanNT Notebook to select a validation exceptions file from a list of files. The file you select appears in the Exceptions file text box.

See also

Using validation / recovery codes

Using the validation exceptions list

The **Files to Exclude from Validation** list on the Exceptions page of the WScanNT Notebook contains the names and locations of files to exclude from validation.

- **Adding.** To add a new file to the list, insert a new line by moving the insertion bar to where you want to add it and pressing *Enter*, then type the name and path of the file you want to add, such as `c:\lotus\123.com`. Alternatively, click the Add button and select the file from a list of files.
- **Changing.** To change a file entry on the list, drag the mouse to select the text you want to change, then type the replacement text.
- **Removing.** To remove a file from the list, drag the mouse to select the entire line, then press *Del* or *Backspace*.

See also

Using validation / recovery codes

Setting the scan frequency

On the Scheduler dialog box, select the frequency interval (Daily, Weekly, or Monthly) with which you want WScanNT to perform automatic scanning.

You can also set the schedule day and time.

Setting the scan date

On the Scheduler dialog box, select the date on which you want to scan.

- If the frequency is **Weekly**, select the day of the week (Sunday through Saturday).
- If the frequency is **Monthly**, select the day of the month (1 through 31).
- If the frequency is Daily, this list is unavailable.

You can also set the schedule frequency and time.

Setting the scan time of day

On the Scheduler dialog box, set the time of day at which an automatic scan will occur (midnight to 11:00 p.m.)

You can also set the schedule frequency and date.

Scanning local drives

Select the **Local Drives** check box on the Scheduler dialog box to scan all local drives on the workstation.

Command line equivalent is /ADL.

Scanning network drives

Select the **Network Drives** check box on the Scheduler dialog box to scan all network drives to which the workstation is currently attached.

Command line equivalent is /ADN.

Selecting items for scheduled scans

Choose the **Select** button on the Scheduler dialog box to select a drives, directories, and files to scan for the currently selected scheduled scan *ONLY*. The items you select are saved when you add the scheduled scan.

You can also choose the Options button to select settings in the WScanNT Notebook.

Selecting items from within the Scheduler dialog box *DOES NOT* change the scanning options currently selected for scanning in the main application.

Selecting options for scheduled scans

Choose the **Options** button on the Scheduler dialog box to display the WScanNT Notebook and select scanning options for the currently selected scheduled scan *ONLY*. The options you select are saved when you add the scheduled scan.

You must also choose the Select button to select drives, directories, and files to scan.

Selecting options from within the Scheduler dialog box *DOES NOT* change the scanning options currently selected for scanning in the main application.

Displaying a list of scheduled scans

This **Active** Schedules list on the Scheduler dialog box displays the scans that are scheduled for the future. Each scheduled scan resides in a separate .INI file.

Choose the Add and Delete buttons to add and remove, respectively, scheduled scans on this list.

Adding a scan to the schedule

Choose the **Add** button on the Scheduler dialog box to add a scan to the schedule.

When you add a scan, WScanNT saves the frequency and options you've set and items you've selected in the WSCANNT.INI file.

Removing a scan from the schedule

Select a scheduled scan in the schedule list, then choose the **Delete** button on the Scheduler dialog box to remove the selected scan from the schedule.

When you delete a scheduled scan, WScanNT removes its entry in the WSCANNT.INI file.

See also

Scheduler dialog box

Closing the Scheduler dialog box

Choose the **Close** button to close the Scheduler dialog box.

Viewing the activity log

The Activity Log dialog box displays the scanning events saved in the activity log file.

Item	Description
Summary of Activities	Displays the most recent scanning events.
Details	Displays items scanned and infections found during the selected event.
Print	Prints the log file.
Clear Log	Deletes the selected items from the log file.

See also

Using the activity log

Viewing the activity log details

The **Activity Log - Details** dialog box displays the items scanned and viruses found during the selected event in the Activity Log dialog box.

Item	Description
Items were scanned	Displays the items scanned for the selected event.
Viruses were found	Displays the viruses found during the selected event.
Print	Prints the detail information in the log file.

See also

Using the activity log

Displaying the virus list

Choose **Scan|Virus List** or click the **Virus List** icon to display a list of viruses that WScanNT detects, identifies, and disinfects. Command line equivalent is /VIRLIST.

The virus list describes the many known viruses that WScanNT detects, identifies, and disinfects. It tells you whether WScanNT can remove the virus and provides additional information about the virus and the files it infects. The virus list information is stored in the NAMES.DAT file. It includes the following information about each virus.

Infects describes what the selected virus infects:

- **Files**, if selected, indicates that the virus infects files. If the virus targets files with specific extensions or files of a specific type, the extensions appear to the right of the check box.
- **Boot Sectors**, if selected, indicates that the virus infects the boot sector of a disk.
- **MBR**, if selected, indicates that the virus infects the master boot record of a disk.
- **Could be Cleaned**, if selected, indicates that WScanNT can remove the virus from infected files.

Features describes behaviors of the selected virus:

- **Memory Resident**, if selected, indicates that the virus is a terminate-and-stay-resident (TSR) program that remains in memory while the computer is running.
- **Encrypted**, if selected, indicates that the virus attempts to evade detection by self-encrypting.
- **Polymorphic Virus**, if selected, indicates that the virus attempts to evade detection by changing its internal structure or its encryption techniques.
- **Virus Size** describes the amount, in bytes, that the virus increases the size of a file it infects.

See also

Searching the virus list

Closing the Virus List

Listing viruses detected by WScanNT

This list on the Virus List dialog box displays the viruses that WScanNT detects, identifies, and disinfects. Scroll through this list using the scroll bars, then choose Close when finished.

Searching the virus list

To quickly find a virus in the virus list, type the first letter of the virus name, then scroll through the list using the scroll bar.

Closing the virus list

Choose **Close** to close the Virus List dialog box.

Loading WScanNT settings from a file

Choose **File|Load Settings** to load WScanNT settings from a settings file. The Load Settings dialog box appears. Select the settings file you want, then choose **OK**.

Command line equivalent is /LOAD.

See also

Using settings files

Saving settings to a file

Choose **File|Save Settings** to save the current WScanNT settings to a settings file. The Save Settings dialog box appears. Enter or select a file name, then choose **OK**.

See also

Using settings files

Selecting a profile

To select a profile, choose **File|Profiles** or click the **Profiles** icon. The Run Profile dialog box appears.

Choose the button of the profile you want. WScanNT loads the associated profile file, then scans your system using those settings.

See also

- Closing the Profiles dialog box
- Using profiles
- Setting up profiles
- Formatting a profile file

Closing the Profiles dialog box

Choose the **Close** button to close the Profiles dialog box.

Using the Selections list

The **Selections** list on the Select Items to Scan dialog box displays a list of selected drives, directories, and files to scan.

You can change this list using the Add Drive, Add Directory, Add File, and Remove buttons.

Adding a file to the Selections list

Select a file you want to add in the **Files** list on the Select Items to Scan dialog box, then choose the Add File button to add it to the Selections list.

Adding a directory to the Selections list

Select a drive you want to add in the **Directories** list on the Select Items to Scan dialog box, then choose the **Add Directory** button to add it to the Selections list.

To scan subdirectories of a selected directory, you must select the Subdirectories check box on the Controls page of the WScanNT Notebook.

Adding a drive to the Selections list

Select a drive you want to add in the **Drives** list on the Select Items to Scan dialog box, then choose the **Add Drive** button to add it to the Selections list.

If you select a drive, its subdirectories are scanned automatically.

Closing the Select Items to Scan dialog box

Choose the **OK** button to save your selections and close the Select Items to Scan dialog box.

Removing an item in the Selections list

Select an item from the Selections list on the Select Items to Scan dialog box, then choose the **Remove** button to remove it from the list.

See also

Select Items to Scan dialog box

Displaying WScanNT version information

Choose **Help|About WScanNT** to display information about the version of WScanNT you are running.

Getting help on Windows help

Choose **Help|Help on Help** to get help on using the Windows help system.

You can also get help by pressing *F1* while using the Windows help system.

Searching for a Help topic

Choose **Help|Search** to search for a topic in WScanNT Help.

Begin scanning your system

Choose **Scan|Start Scan** or click the **Scan** icon to begin scanning based on the items and settings you have selected.

Before scanning, you must select the drives, directories, and files you want to scan. See File|Select Items to Scan.

Printing the activity log

Choose the **Print** button on the Activity Log dialog box to print the activity log.

The Print dialog box appears. Select the options you want, then choose **OK**.

See also

Using the activity log

Printing the activity log details

Choose the **Print** button on the Activity Log - Details dialog box to print details of the activity log.

The Print dialog box appears. Select the options you want, then choose **OK**.

See also

Using the activity log

Printing the virus list

Choose the **Print** button on the Virus List dialog box to print the contents of the virus list.

The Print dialog box appears. Select the options you want, then choose **OK**.

Printing a report of scan results

Choose the **Print Reports** button on the main WScanNT window to print a report of scan results.

The Print dialog box appears. Select the options you want, then choose **OK**.

Setting up the printer

Choose **File|Print Setup** to set up the printer. Select the options you want, then choose **OK**.

Printing the scan log

Choose **File|Print** or click the **Print** icon to print a report of scan results.

You can also set up the printer before printing.

Setting up the printer

Choose **File|Print Setup** to select a printer, page orientation, and paper size and source before printing. Select the options you want, then choose **OK**.

Exiting WScanNT

Choose **File|Exit** to exit WScanNT.

If you've changed settings, WScanNT asks you whether you want to save them. If you answer **Yes**, WScanNT will save them.

WScanNT Glossary

AGENTS.TXT

A text file that contains the names of all McAfee authorized agents.

America Online technical support

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 email to **MCAFEE**.

Authorized Agents (overseas only)

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

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

archived file

A file that has been archived using either LZEXE or PKLITE, file compression utilities.

AUTOEXEC.BAT

Batch (command) file containing DOS commands that are executed automatically when the computer is started or restarted.

backup

A safe copy of programs or data, in case the original copy is lost or damaged.

McAfee BBS

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 14,400 bps with line settings of 8 data bits, no parity, and 1 stop bit.

boot

To start a computer. The first step is to load startup instructions from the boot ROM or boot sector of a disk.

boot ROM

A read-only memory chip that contains the coded instructions for the operating system to start the computer. Often present in portable computers, a boot ROM is not susceptible to infection (unlike the boot sector on a disk). However, it is harder to update.

boot sector

A portion of a disk that contains the coded instructions for the operating system to start the computer.

boot sector infections

Contamination of the boot sector by a virus. Particularly serious because information in the boot sector is loaded into memory first, before virus protection code can be executed. The only certain way to eliminate boot sector infections is to restart from a disk known to be uninfected, then clean up the infection.

clean startup diskette

A diskette known to be uninfected, that contains the coded instructions from which the computer can be started. See Chapter 2 for instructions on preparing one.

CLEAN.DAT

A file that contains the virus recovery information that Scan uses to recover infected files.

cold boot

To start a computer from power-off state.

compressed file

A file (usually with a .ZIP extension) that has been compressed using the PKZIP file compression utility.

CompuServe technical support

We sponsor the McAfee Virus Help Forum on CompuServe. To reach it, type `GO MCAFEE` at any CompuServe prompt. A free introductory membership is available. For more information, please read the COMPUSER.TXT file on your disk.

CONFIG.SYS

A file that lists device drivers and other configuration parameters that are automatically loaded when the computer is started or restarted.

conventional memory

Up to 640K of main memory in which DOS executes programs.

corrupted file

A file that has been damaged. About 10% to 20% of viral infections involve viruses that damage files beyond repair.

critical virus

A virus that can cause catastrophic damage or spread an infection during a scan.

detection

Scanning memory and disks for telltale marks or changes indicating that a virus might be present.

disinfect

To eradicate a virus so that it can no longer spread or cause damage to a system.

download

To retrieve a file from a remote computer system.

ERRORLEVEL

A DOS variable that can be set by a program as it terminates to indicate an error condition. A batch (command) file can read the ERRORLEVEL and take appropriate action.

exception list

List of files to which validation codes should not be added because they are already immunized against viruses or contain self-modifying code. Scans /AV option uses the list to avoid adding codes to inappropriate files; VShields /CERTIFY option can use it to allow certain unvalidated files to be run.

executable (file)

A file containing coded instructions to be executed by the computer. Executable files include programs and overlays.

expanded memory

Memory above DOSs 640K limit of conventional memory that is accessed by memory paging. You need special software, conforming to an expanded memory specification, to take advantage of expanded memory.

extended memory

Linear memory above DOSs 640K limit of conventional memory. Often used for RAM disks and print spoolers.

false alarm

Detecting a virus when none is present.

infected file

A file contaminated by a virus.

infection

Contamination of a computer system by a virus.

Internet support (mcafee.com)

The latest versions of McAfee's anti-virus software are available by anonymous ftp (file transfer protocol) over the Internet from the site mcafee.com. If your domain resolver does not support names, use the IP# 192.187.128.1. 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 email to **support@mcafee.com**.

You can also find McAfees 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)

master boot record (MBR)

A portion of a hard disk that contains a partition table that divides the drive into chunks, some of which may be assigned to operating systems other than DOS.

McAfee

Founded in 1989, McAfee is the leading provider of tools for productive computing for the 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 downloaded from bulletin board systems and on-line services around the world.

McAfee updates the VirusScan programs every 6 - 8 weeks or more to add new virus detectors, new options, and fix reported bugs. 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 more than 50 countries worldwide.

memory

A storage medium where data or program code are kept temporarily while being used by the computer. DOS supports up to 640K of conventional memory. Beyond that limit may be accessed as expanded memory, extended memory, or an upper memory block (UMB).

memory infection

Contamination of memory by a virus. The only certain way to eliminate memory infections is to restart from a disk known to be uninfected, then clean up the source of infection.

modified file

A file that has changed after validation / recovery codes have been added.

NetShield[a]

A protection program that detects viruses on a NetWare server.

network

A linkage of computers so that they can communicate and share information and resources.

overlay infection

Virus contamination of a file containing auxiliary program code that is loaded by the main program.

partition table

See master boot record.

polymorphic virus

Virus that attempts to evade detection by changing its internal structure or its encryption techniques.

program

Software that performs a defined function on a computer. See executable.

read operation

Any operation in which information is read from a disk. DOS commands that perform read operations include **dir** (directory listing), **type** (display contents of a file), and **copy** (copy files).

See also write operation.

README.1ST

Text file that contains manual updates and late-breaking instructions for the current version of the program.

recovery codes

Information that Scan records about an executable file in order to recover if it is infected by a virus. See also *validation codes*.

Scan

McAfees command line program that detects and disinfects viruses from your system.

SCAN.EXE

Scan program file for DOS.

SCAN.DAT

Data file used by Scan to detect known viruses.

WSCANNT.LOG

File in which Scan records the date and time of the last scan conducted.

secure environment

A setting in which high security against virus infection is important.

security program

An organized system of safety measures and procedures, designed to protect a computing environment against loss or theft of software, data, productivity, and proprietary information.

self-modifying program

Software that deliberately changes its own program file, often to protect against viruses or illegal copying, and is therefore difficult to validate in conventional ways.

standard extensions

Filename extensions (suffixes) that signify executable files - EXE, COM, SYS, DLL, BIN, OVL - which Scan checks by default. (Note that these extensions have changed from earlier versions).

sterile field

In medicine and, by analogy, computing, a work area that is known to be infection-free. To maintain the field, foreign objects (files) brought into the field must be sterilized first.

subdirectory

Like a file folder, a location on a disk where files (and possibly other folders) are stored.

Summary window

A screen area that shows the results of a scan, including infections, warnings, and errors.

system errors

Errors that can prevent Scan from completing its job successfully. System error conditions include disk format errors (such as unformatted disks), media errors (bad sectors), file system errors (unreadable files), network errors (unable to log in), file access errors (access permission denied), device access errors (printer out of paper), and report failures.

turbo

A scanning option that is faster than normal but less comprehensive (because it checks a smaller portion of each file).

unknown virus

A virus not yet identified and listed in SCAN.DAT. VirusScan can detect unknown viruses by observing changes in files that could result from infection.

upper memory block (UMB)

Memory in the range 640 - 1024K, just above DOS's 640K limit of conventional memory.

validate

To check that a file is authentic and has not been altered. Most validation methods rely on computing a statistic based on all the data in the file, which is unlikely to remain constant if the file itself is changed.

VALIDATE.EXE

A DOS program that verifies the authenticity of McAfee software.

validation codes

Information that Scan records about an executable file in order to detect subsequent infection by a virus. See also recovery codes.

virus

A software program that attaches itself to another program in computer memory or on a disk, and spreads from one program to another. Viruses may damage data, cause the computer to crash, display messages, or lie dormant.

virus-free environment

A setting that is known to be clean and uninfected.

warm boot

To restart (reset) a running computer, in DOS by pressing [Ctrl]-[Alt]-[Del].

write operation

Any operation in which information is recorded on a disk. Commands that perform write operations include those that save, move, and copy files. Most write operations are also read operations because the system verifies that the data have been written correctly.

See also read operation.

write protection

A mechanism to protect files or disks from being changed. A 3.5 diskette may be write-protected by sliding its corner tab so that the square hole is open; a 5.25 diskette by covering its corner notch with a write-protect tab. A file may be write-protected by changing its system attributes.

WSCANNT.EXE

Scan program file for Windows NT.