Using VirusScan NT

Overview

This chapter contains general information about VirusScan NT's virus detection and removal capabilities. For more detailed information about this product, refer to Chapter 4, "VirusScan NT Technical Reference."

Running NTScan

VirusScan NT examines your PC and disks for viruses. The first time you run NTScan, do so from the original, write-protected diskette so that the programs themselves cannot be infected.

This section contains all the information most users of NTScan will need. More detailed information is available in Chapter 4, "VirusScan NT Technical Reference."

Launching NTScan

Always start NTScan from the DOS prompt (C:\) by launching a Windows 32-Bit Dos Command prompt.

✍ *The \MCAFEE\VIRUSCAN directory should be identify in your search path. If necessary, go to the Control Panel and add the directory to your path statement.*

Use the following syntax for NTScan:

```
ntscan {drives} [options]
```

ntscan launches the application.

{drives} indicates one or more drives to be scanned. You must specify at least one drive to be scanned. If you specify a drive with just the drive letter and a colon (e.g. **ntscan c:**), all its subdirectories will be scanned. If you specify only a back-slash (e.g. **ntscan **), only the root directory of the active drive will be scanned. You can also scan a specific directory (e.g. **ntscan c:\mcafee**).

[options] indicates one or more of the NTScan options. The following section, “NTScan Command Line Options,” lists some of the more commonly-used NTScan command line options. A full listing and a more detailed explanation of each option is presented in “NTScan Command,” in Chapter 4, “VirusScan NT Technical Reference.”

NTScan command line options

/? or /HELP

Does not scan. Instead, displays a list of NTScan command line options with a brief description of each. No scanning is performed when these options are specified. Use either of these options alone on the command line, for example:

```
ntscan /?
```

This command will return a full listing of NTScan's command line options, pausing when the screen is full. This listing is also available in Chapter 4, "VirusScan NT Technical Reference."

/ADL

Scans all local drives (including hard drives, compressed, CD-ROM and PCMCIA drives, but not diskettes) for viruses, in addition to those specified on the command line. To scan both local and network drives, use /ADL and /ADN together in the same command line; for example:

```
ntscan /adl /adn
```

NTScan will check all local drives and network drives for viruses.

/ADN

Scans all network drives for viruses, in addition to those specified on the command line. To scan both local and network drives, use /ADL and /ADN together in the same command line. Refer to /ADL for an example of using this command.

/ALL

Increases system security by performing a more thorough scan. By default, NTScan checks only standard executable files (with .COM, .EXE, .SYS, .BIN, .OVL and .DLL extensions), which are the files most likely to be infected by a virus. If /ALL is specified, NTScan checks all files on the specified drive, which increases NTScan's ability to detect viruses in overlay files but substantially increases the scanning time required.

For example:

```
ntscan a: /all /clean
```

The above command line will check all files on A: drive and will attempt to restore any infected files.

Use this option if you have found a virus or suspect one, or if you operate in a highly-vulnerable environment.

/CLEAN

Remove viruses from boot sector, master boot record and infected files.

Attempts to restore the boot sector (if infected) and any infected files. Usually, between 10% and 20% of all viruses are not removable; they damage the file they infect beyond repair. If the infected file resides on a network drive, you must have rights to modify files on that drive to clean it. If it cannot restore a file, a message is displayed that identifies the unrecoverable file. To use /CLEAN, the CLEAN.DAT file must reside in the same directory as NTSCAN.EXE. For more information, refer to "Removing viruses" in Chapter 4, "VirusScan NT Technical Reference."

Consider the following command line:

```
ntscan c: /clean
```

NTScan will search for viruses on C: drive and, if infected files or boot sectors are detected, will attempt to restore them.

The /CLEAN option can remove master boot record and boot sector viruses. If you use /CLEAN and /DEL in the same command line, NTScan first attempts to disinfect an infected file, then deletes it only if it cannot be repaired. Similarly, if you use /CLEAN and /MOVE in the same command line, NTScan first attempts to clean an infected file, then moves it to the specified subdirectory if the file is unrecoverable.

✍ *When scanning a network drive using /CLEAN, you must have sufficient rights to update files on that drive.*

/DEL

Overwrite and delete infected files.

Deletes and overwrites each infected file. Files erased by the /DEL option cannot be recovered (you should generate a report so that you can restore them from backups). Instead of using /DEL alone, we recommend using it in combination with the /CLEAN option to attempt to disinfect an infected file first, then delete it only if the file is unrecoverable. The /CLEAN option can remove master boot record and boot sector viruses, but the /DEL option cannot.

```
ntscan a: /clean /del /report c:\mcafee\infected.log
```

NTScan will attempt to restore any infected files on A: drive, then delete any files which could not be cleaned. The results of scanning, including the names of any restored or deleted files, will be saved to the report file “INFECTED.LOG” in the directory C:\MCAFEE.

When scanning a network drive using /DEL, you must have sufficient access rights to delete files on that drive.

✍ *Using /MOVE and /DEL in the same command line returns an error message.*

/FAST

Reduces scanning time by about 15%. Using the /FAST option, NTScan examines a smaller portion of each file for viruses, although it examines more files overall. Using /FAST might miss some infections found in a more comprehensive (but slower) scan. For example:

```
ntscan c:\data /fast
```

This command will perform a “fast scan” on the directory DATA on C: drive.

Do not use this option if you have found a virus or suspect one.

/MANY

Scans multiple diskettes consecutively in a single drive. NTScan will prompt you for each diskette. Once you have established a virus-free system, use this option to check multiple diskettes quickly.

For example:

```
ntscan a: /many
```

Use this line command to scan floppy disks inserted into the A: drive.

/MOVE {directory}

Move infected files to the specified directory.

Moves all infected files found during a scan to the specified directory. If you use /MOVE in conjunction with /CLEAN, NTScan attempts to restore an infected file first, then moves it to the specified directory only if the file cannot be restored. Consider the following example:

```
ntscan c: /clean /move d:\infected
```

NTScan will attempt to restore any infected files, then move any files which could not be cleaned to the directory INFECTED on D: drive.

✍ *Using /MOVE and /DEL in the same command line returns an error message.*

/REPORT {filename}

Saves the output of NTScan to filename in ASCII text file format. If *filename* exists, /REPORT erases and replaces it (or, if you also use /APPEND, adds the report information to the end of the existing file). You can include the destination drive and directory; for example, consider the line command

```
ntscan a: /report d:\vsreprt\all.txt
```

This will scan the floppy drive (A:) and create a report file called “ALL.TXT” on D:\VSREPRT. However, if the destination is a network drive, you must have rights to create and delete files on that drive. You can also use /RPTCOR, /RPTMOD and /RPTERR to add corrupted files, modified files and system errors to the report.

/RPTCOR

Used in conjunction with /REPORT, adds the names of corrupted files to the report file. A corrupted file is a file that a virus has damaged beyond repair, which typically occurs in 10% to 20% of all viral infections. For example, consider the line command

```
ntscan c: /report /append /rptcor c:\mcafee\report.txt
```

This will scan the hard drive (C:) and save the scanning results and the names of any corrupted files to a text file called “REPORT.TXT” in the MCAFEE subdirectory on C: drive. If “REPORT.TXT” already exists, the information will be appended (added) to the existing file.

✍ *You can use /RPTCOR with /RPTMOD and /RPTERR on the same command line.*

/RPTERR

Used in conjunction with /REPORT, adds system errors to the report file. System errors include problems reading or writing to a diskette or hard disk, file system or network problems, problems creating reports and other system-related problems. You can use /RPTERR with /RPTCOR and /RPTMOD on the same command line. Refer to /RPTCOR for an example of using this command.

/RPTMOD

Used in conjunction with /REPORT, adds the names of modified files to the report file. Scan identifies modified files when the validation/recovery codes do not match (using the /CF or /CV options). You can use /RPTMOD with /RPTCOR and /RPTERR on the same command line. Refer to /RPTCOR for an example of using this command.

/SUB

By default, when you specify a directory to scan rather than a drive, NTScan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories inside any directories you have specified; for example:

```
ntscan c:\games /sub
```

This line command will scan all the files in the directory GAMES and its associated subdirectories on the C: drive.

Do not use /SUB if you are scanning an entire drive, as NTScan will automatically scan all directories and subdirectories on that drive.

Using NTScan to detect a virus

Always start NTScan from a DOS prompt (C:\) by launching a Windows 32-Bit Dos Command Prompt.

✍ *The \MCAFEE\VIRUSCAN directory should be identify in your search path. If necessary, go to the Control Panel and add the directory to your path statement.*

After typing each entry on the command line, press [ENTER]. If you include the /REPORT {filename} option, NTScan saves a report of infected files and any system errors to the specified log file. The /ALL option will scan all files, not just standard executables.

1. Insert the write-protected VirusScan program diskette in drive A.

2. Scan your C drive for known viruses by typing:

   a: ntscan c: /report c:\virus.log /all

   If you have more than one hard drive, add them to the scan in the same manner. For example, if you have C and D drives, type:

   a: ntscan c: d: /report c:\virus.log /all

   You can also scan all local drives (including compressed, CD-ROM and PCMCIA drives but not diskettes) using the /ADL option. For example:

   a: ntscan /adl /report c:\virus.log /all

It may take several minutes for the NTScan program to check for viruses in memory, then on the system and user portions of your drives. NTScan keeps you informed of its progress. Read the information on the screen carefully. On the next page is a sample of what NTScan reports when checking a drive for viruses.

```
Virus data file V2.2.9507 created 07/13/95 14:14:43
No viruses found in memory.
Scanning C:
Summary report on C:
```

```
File(s)
        Analyzed:.......          1500
        Scanned:........           750
        Possibly Infected:.......    0
        Master Boot Record(s):..     1
        Possibly Infected:.......    0
        Boot Sector(s):.........     1
        Possibly Infected:.......    0
Time: 60.00 sec.
```

- **Analyzed** indicates how many files NTScan has found on your system.
- **Scanned** indicates how many files NTScan has scanned for viruses. If you are using the default scanning settings, Scan will only check executable files. To check all files, use the /ALL command line option. For more information about setting command line options, refer to Chapter 4, “VirusScan NT Technical Reference.”
- **Possibly infected** indicates how many infected files NTScan has found.

3. If NTScan reports “No viruses found,” congratulations — most likely your system is currently virus-free. Copy any important or critical files to fresh diskettes or tape back up so you will have current, clean files should a virus later infect your system and damage your work. Refer to “Back Up Your Hard Drive” in Chapter 2, “Installation and Setup.”

If NTScan finds one or more viruses, a message similar to the following is displayed:

```
Scanning C:

Scanning file C:\DOS\ATTRIB.EXE

Found the Jerusalem Virus
```

Do not panic, even if the virus has infected many files. At the same time, do not run any other programs, especially if the virus is found in memory. Refer immediately to “Using NTScan to Remove a Virus” in the next section.

4. After scanning your hard drive(s) and other drives, you should scan **all** the diskettes you use with the /MANY option. Insert a diskette into drive A: and type the following command:

```
ntscan a: /many /report c:\virus.log /all
```

NTScan will check the diskette in drive A: and then prompt you to insert the next diskette with the message:

```
Please replace the media and press any key to scan
it. (ESC to exit)
```

Insert the next diskette into A: and press any key to continue scanning. Continue until you have scanned all of your diskettes. When you are finished, press the ESC key.

If VirusScan finds a virus, refer immediately to “Using Scan to Remove a Virus” in the next section.

✍ *The NTScan program files should be on a drive that is not removed. For example, an error may result if you use the command line*

```
a: ntscan a: /many
```

Perform the scan from a drive that is not to be removed (i.e. scan A: drive from C: drive or B: drive).

Using NTScan to remove a virus

If you detect a virus, you can run NTScan with the /CLEAN option to eradicate most known viruses from your disks. If you are at all unsure about how to proceed once you have found a virus, contact McAfee for assistance (refer to "McAfee Support" in Chapter 1, "Introducing VirusScan NT").

If VirusScan detected a Master Boot Record (MBR) or Boot Sector virus, you will have to remove the virus using the procedure outlined in "If install detects a virus" in Chapter 2, "Installation and Setup."

✍ **WARNING!** *Using DOS commands (i.e. FORMAT, FDISK, DEBUG) from a Windows 32-Bit Dos Command Prompt to remove a virus can result in the* ***loss of all data and use of the infected disks****. If you are unfamiliar with viruses and virus methodology, contact McAfee immediately for assistance before using DOS commands to remove a virus (refer to "McAfee Support" in Chapter 1, "Introducing VirusScan NT"). For more information, refer to "Using DOS commands to remove a virus" in Chapter 5, "Tips and Troubleshooting."*

NTScan has options to control and fine-tune the scope, validation and operation of its disinfection. For details, refer to Chapter 4, "VirusScan NT Technical Reference."

Master Boot Record and Boot Sector Viruses

If VirusScan has detected a Master Boot Record (MBR) or Boot Sector virus, follow the procedures outlined in "If install detects a virus"Chapter 2, "Installation and Setup." Do not attempt to remove a Master Boot Record or Boot Sector virus using NTScan.

Run NTScan with the /CLEAN option

If VirusScan NT has detected one or more infected files, use NTScan to remove the virus.

Step	Action
1.	Launch a Windows 32-Bit Dos Command Prompt.

2. Remove the first known virus on all local drive(s) (including hard drives, compressed, CD-ROM and PCMCIA drives, but not diskettes) by typing:

```
ntscan /adl /clean /all /report c:\infectd.txt
```

NTScan keeps you informed of its progress and generally reports virus removed successfully. If the virus was successfully removed, refer to "If Viruses Were Removed," below. If NTScan reports that the virus could *not* be safely removed, refer to "If Viruses Were Not Removed" on page 44.

If the virus was detected on a diskette, insert the diskette into drive A: and type:

```
ntscan a: /many /clean /all /report c:\infectd.txt
```

NTScan will check the diskette in drive A: and, if a virus is present, will remove the virus if possible. If NTScan reports that the virus has been successfully removed, remove the diskette from the drive, insert the next diskette and press any key. If NTScan reports that the virus could not be safely removed, remove the diskette from the drive, indicate that it is still infected by marking the label, insert the next diskette and press any key. After scanning all your diskettes, perform the procedure in "If Viruses Were Not Removed" on page 44 on any disks that could not be successfully cleaned.

✍ *The VirusScan program files should be on a drive that is not removed. For example, an error may result if you use the command line*

```
a: ntscan a: /many
```

Perform the scan from a drive that is not to be removed (i.e. scan A: drive from C: drive or B: drive).

If Viruses Were Removed

If NTScan successfully removes all the viruses, restart your computer. Run NTScan again to verify that your system is now virus-free. Be sure to examine and disinfect any diskettes you use as well, as diskettes are a common source of virus infection. Refer to "Rescaning new disks and software" in Chapter 2, "Installation and Setup."

If Viruses Were Not Removed

If NTScan cannot remove a virus, it will tell you:

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

Make sure to take note of the filename, because you will need to restore it from backups. Run NTScan again, this time using the /CLEAN and /DEL options to delete the remaining infected files, as described in "NTScan command line options" on page 33 and in Chapter 4, "VirusScan NT Technical Reference." If you have any questions, contact McAfee (refer to "McAfee Support" in "Introducing VirusScan NT").

False Alarms

Due to the nature of anti-virus software, there is a possibility that VirusScan may report a virus in a file or in memory, even if a virus does not exist. 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 rather than on the boot disk.

Always assume that the virus is genuine. Follow the procedures outlined in "Using NTScan to remove a virus" on page 42. After you have performed these procedures, if you still feel that the virus alert was a "false alarm" please contact McAfee (refer to "McAfee Support" in Chapter 1, "Introducing VirusScan NT"). You can upload the file to our bulletin board system at (408) 988-4004, along with your name, address, daytime telephone number and electronic mail address (if any).

For more information, refer to "False alarms" in Chapter 5, "Tips and Troubleshooting."

Using DOS Scan to remove a virus

If you detect a master boot record or boot sector virus, you can run DOS Scan with the /CLEAN option to remove the virus. If you are at all unsure about how to proceed once you have found a virus, contact McAfee for assistance (refer to "McAfee Support" in Chapter 1, "Introducing VirusScan NT"). You can also use DOS scan to remove viruses that have infected files on your system.

✍ **WARNING!** *Using DOS commands (i.e. FORMAT, FDISK, DEBUG) to remove a virus can result in the* ***loss of all data and use of the infected disks****. If you are unfamiliar with viruses and virus methodology, contact McAfee immediately for assistance before using DOS commands to remove a virus (refer to "McAfee Support" in Chapter 1, "Introducing VirusScan NT"). For more information, refer to "Using DOS commands to remove a virus" in Chapter 5, "Tips and Troubleshooting."*

DOS Scan has options to control and fine-tune the scope, validation and operation of its disinfection. For details, refer to "Using DOS Scan to remove a virus" in Chapter 4, "VirusScan NT Technical Reference."

Restart from a clean environment

Restart your computer from a diskette you know to be virus-free, preferably the original write-protected DOS installation diskette that came with your computer. If you do not have one, get one from someone else; do not use a diskette that might be infected. (If you do not have one, you can create one following the procedure outlined in "Creating a clean DOS start-up diskette", but only *after* you have successfully cleaned your system.)

Step	Action
1.	Shutdown your computer. (Do not just reset or reboot, since doing this may leave some viruses in your computer's memory.)
2.	Make sure your clean DOS boot (start-up) diskette is write-protected.

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

- For a 5.25” diskette, cover its corner notch with a write-protect tab. Be sure to use the write-protect stickers provided with your diskettes, not tape.

3. Insert your DOS start-up diskette in drive A and restart your computer.

4. You should see a DOS prompt (A:\). Do not run any other programs or you risk spreading a virus.

5. Remove the DOS start-up diskette.

Run DOS Scan with the /CLEAN option

Step	Action

1. Insert the diskette containing the DOS version of Scan into drive A. This diskette was included with your VirusScan package. If you downloaded VirusScan NT from the McAfee BBS, run DOS Scan from the directory on your hard drive you downloaded the VirusScan program files to.

2. Make sure your DOS Scan diskette is write-protected.

   - For a 3.5" diskette, slide its corner tab so that the square hole is open.
   - For a 5.25" diskette, cover its corner notch with a write-protect tab. Be sure to use the write-protect stickers provided with your diskettes, not tape.

3. Eliminate the first known virus by searching all files on all local drive(s) (including hard drives, compressed, CD-ROM and PCMCIA drives, but not diskettes) by typing:

   ```
   scan /adl /clean /all
   ```

After typing each entry on the command line, press [ENTER].

Scan keeps you informed of its progress and generally reports virus removed successfully.

- If Scan reports that the virus was successfully removed, refer to “If viruses were removed” on page 47.

- If Scan reports that the virus could not be safely removed, refer to "If viruses were not removed," below.

If viruses were removed

If Scan successfully removes all the viruses, restart your computer. Begin the installation procedure again as described in "Installing VirusScan NT" in Chapter 2, "Installation and Setup." Install will again scan your system and, assuming your system is now virus-free, will install VirusScan.

One common source of virus infection is diskettes. Once you have finished installing VirusScan on your hard disk, use Scan again to examine and disinfect all the diskettes you use, as described in "Rescaning new disks and software"Chapter 2, "Installation and Setup."

If viruses were not removed

If Scan cannot remove a virus, it will tell you:

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

Make sure to take note of the filename, because you will need to restore it from back-ups. Run Scan again, this time using the /CLEAN and /DEL options to delete the remaining infected files, as described in Chapter 4, "VirusScan NT Technical Reference."

One common source of virus infection is diskettes. Once you have finished installing VirusScan on your hard disk, use Scan again to examine and disinfect all the diskettes you use, as described in "Rescaning new disks and software"Chapter 2, "Installation and Setup."