Tips and Troubleshooting

Overview

The other chapters in this manual are meant to tell you clearly and concisely how to use the VirusScan NT software. Still, you may have questions or encounter confusing situations. This chapter contains two kinds of advice:

- Tips for getting the most out of VirusScan NT.
- Common problems and how to solve or avoid them.

If this information does not help resolve your question or problem, contact McAfee (refer to "McAfee Support" in Chapter 1, "Introducing VirusScan NT").

Tips

Creating a virus-free environment

- Be sure to follow the installation procedures as outlined in Chapter 2, “Installation and Setup.”
- Scan **all** the diskettes you use by using NTScan with the /MANY option (refer to “Using NTScan to detect a virus” in Chapter 3, “Using VirusScan NT.”). Never start your computer from an unknown diskette. Always make sure your disk drive(s) are empty before turning on or restarting your computer.
- Rescan whenever you introduce new programs onto your computer. Run VirusScan NT on a new diskette before executing, installing or copying its files onto your system. If you download or install software from a network server, bulletin board or on-line service, always run VirusScan on the directory you placed the new files in before executing them.
- Create a DOS start-up diskette containing the NTScan program by following the procedure outlined in Chapter 2, “Installation and Setup.” Make sure this disk is write-protected so that it cannot become infected.

Detecting new and unknown viruses

There are two ways of dealing with new and unknown viruses that may infect your system:

- Update VirusScan NT regularly.
- Store and check validation and recovery information about your files.

Update VirusScan regularly

Most likely, McAfee will see new viruses long before you do. We update the VirusScan programs often — usually monthly, but more often if many new viruses have appeared. Each new version may detect and eradicate as many as 60 to 100 new viruses or more, and may fix bugs that have been reported.

Updating VirusScan NT regularly is probably all you need to do to protect against new viruses. Refer to the instructions for obtaining new versions in "Update VirusScan regularly," in Chapter 2, "Installation and Setup."

Use the validation and recovery options

If your environment is highly vulnerable to viruses, or you require unusual security against them, you can use VirusScan's validation and recovery options. Scan 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 NTScan reports that the file may have become infected. Scan has two levels of validation, which are stored in two separate ways:

- It can store the enhanced code in a separate recovery file, which can be stored off-line (for example, on a diskette) for recovery purposes (/AF, /CF and /RF switches). This is the preferred method because it stores recovery data in a separate file.

- It can append a simple 98-byte validation code to .COM and .EXE files (/AV, /CV and /RV switches). This method applies to the files you specified only.

Once the validation codes are stored, VirusScan can use the /CV and /CF options to detect changes to the files. More importantly, if you have stored the recovery information with /AF, VirusScan can use it to restore infected files.

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 / RV or /RF options to remove all codes, then /AV or /AF to restore them.

If you want to use one of these methods, which should you use? We recommend the "F" options — /AF, /CF, and /RF — over the "V" options. /AF stores the validation and recovery information in a separate file, instead of modifying the program files themselves. This has the following advantages:

- 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) and access it on demand to check for, and recover from, infection by unknown viruses. Use the procedure below to create a recovery diskette.

- This method keeps self-checking files (usually copy-protected programs) from reporting that they have been tampered with.

✍ *If you use this method, you do not need an exception list. However, it is important that you run NTScan 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.*

✍ *The "V" options are primarily useful for companies that distribute software to their customers or employees, and want to incorporate an additional level of virus protection.*

Developing a security program

VirusScan has been shown to be an effective virus-preventive measure when used in a conscientiously applied program of network security and regular professional care.

VirusScan is one important element of a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training and awareness. Even with VirusScan, some viruses— not to mention theft or fire — can render a disk unrecoverable without a recent backup. Although outlining such a security program is beyond the scope of this manual, refer to "Other sources of information," in Chapter 1, "Introducing VirusScan NT," for suggestions.

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

Interacting with your network

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

Run Scan on network drives

Run from a workstation (PC) on the network, VirusScan checks network drives for viruses just as it does local drives. For convenience, the /ADN option scans all network drives to which the workstation is connected.

Use NetShield

NetShield 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. On other kinds of networks, you can use Scan to check network servers.

Using a recovery diskette

To store the recovery file on the clean startup diskette you created in "Creating a clean DOS start-up diskette," in Chapter 2, "Installation and Setup," temporarily remove write-protection from the diskette and insert it in drive A. Run NTScan on your hard disks with the /AF option. For example, launch the Windows 32-Bit Dos Command prompt to display a "DOS" prompt (C:\) and type:

```
ntscan /adl /af a:\scancrc.crc
```

This command will scan the local hard disk drives (including compressed, CD-ROM, and PCMCIA drives, but not diskettes) for known viruses and create SCANCRC.CRC, a file containing recovery data and validation codes, on the diskette. After NTScan finishes, write-protect the diskette.

To check for virus infection, turn your computer off, insert the write-protected recovery diskette in drive A and turn the power back on. The PC will now start from the diskette. Launch the Windows 32-Bit DOS Command Prompt to display the DOS prompt (C:\) and type:

```
ntscan /adl /cf a:\scancrc.crc
```

VirusScan will compare the local hard disk drives against the recovery data stored on the diskette in the SCANCRC.CRC file.

If you detect an unknown virus, to disinfect your system, turn your PC off, insert the write-protected recovery diskette and turn the power back on. The PC will start from the diskette. Launch the Windows 32-Bit Dos Command Prompt and type:

```
ntscan /adl /cf a:\scancrc.crc /clean
```

VirusScan will restore local hard disk drives (including CD-ROM and PCMCIA drives) with the recovery data stored in SCANCRC.CRC on the diskette.

If you install new software, or upgrade your Windows NT version, remember to update your recovery file. Refer to “Use the validation and recovery options” on page 83.

Troubleshooting

Failed integrity check

NTScan performs an integrity test before running. This self-check allows NTScan to determine if it has been modified. If NTScan fails its integrity test, a warning message appears, and NTScan refuses to run and returns to the command line prompt.

NTScan may report a "false" failed integrity check if you upgrade VirusScan's data files and perform an immediate NTScan. After upgrading VirusScan, turn off your computer, wait a few seconds and turn it on again. Refer to "Update VirusScan regularly," in Chapter 2, "Installation and Setup."

If you did not upgrade VirusScan files and receive a failed integrity check warning, your VirusScan program files may have been corrupted or damaged. Obtain an undamaged copy of VirusScan from a known source. Refer to "McAfee Support" in Chapter 1, "Introducing VirusScan NT."

False alarms

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 VirusScan may "detect" them falsely as a virus. Your system's BIOS, use of validation codes and other factors may also produce false alarms. **Always assume that any virus found by VirusScan is a real and dangerous virus,** and follow the procedures as outlined in Chapter 3, "Using VirusScan NT." That is, turn off your computer and reboot from a known clean start-up disk; launch the Windows 32-Bit DOS Command Prompt; run Scan again with the /ADL and /ALL switches from a write-protected diskette; and clean any infected files that Scan detects using the /CLEAN command. If you have any questions, contact McAfee immediately (refer to "McAfee Support" in Chapter 1, "Introducing VirusScan NT").

If, after following the procedures outlined above, you believe that VirusScan is falsely detecting a virus, refer to the list below of potential sources of false alarms:

- Set up your computer so that only one anti-virus program is running at a time. Remark out lines in the AUTOEXEC.BAT that refer to other anti-virus programs, such as VSafe. **Turn off** your computer, wait a few seconds and turn it on again to make certain all code from other anti-virus programs are cleared.

  ✍ *Your computer's BIOS may include an anti-virus feature. The only way to disable this feature is to remove it from your CMOS file.*

  We make every attempt to prevent false alarms, but some viruses can only be detected in a very limited way. This is a reason two anti-virus programs can cause false alarms.

  If the virus warning is only on one file that has been used for years and is not on any other files, it may be a false alarm. Please contact McAfee or send the file to us for analysis.

- If you set up validation codes, subsequent scans can detect changes in validated files. This can trigger 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. For more information, refer to "Option details," in Chapter 4, "VirusScan NT Technical Reference."

- Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. If you are using the /AF or /CF switches, Scan will report that the boot sector has been modified, even though no virus may be present. Check your system's reference manual to determine whether your PC has self-modifying boot code. To solve this problem, use the /AV and /CV switches instead (which do not check the system area for changes).

- If the virus is only found in memory and only when booted from the hard drive, it is most likely a false alarm. MEM should read 640K or 655,360 total conventional memory. Contact technical support if you are unsure (refer to "McAfee Support" in Chapter 1).

- NTScan may incorrectly report viruses in the boot sector or master boot record of certain copy-protected diskettes. Contact technical support if you are unsure (refer to "McAfee Support" in Chapter 1, "Introducing VirusScan NT").

Installation failure

The installation may fail if you are running another anti-virus program during the install procedure. Be sure that all other anti-virus programs are unloaded from memory before beginning the install procedure. Refer to Chapter 2, “Installation and Setup.”

Using DOS commands to remove a virus

Before you use a DOS command (e.g. FORMAT.COM, FDISK.EXE, SYS.COM or DEBUG.EXE) to attempt to remove a virus, contact McAfee immediately for experienced help.

Using DOS commands to remove viruses or clean virus-infected files can result in the loss of all data and the use of infected disks. The common viruses Stoned and Monkey, for example, can destroy the master boot record and all data on the disk if removed improperly with DOS commands. Other viruses will damage or overwrite program (.EXE) files or overlay files, and attempts to remove these viruses with DOS commands can damage or destroy the files.

It is very dangerous to attempt to remove any virus, or to clean a virus-infected file, with DOS commands. If you are unfamiliar with viruses and virus methodology, you should get experienced help before using DOS commands to avoid losing data, programs or disks. For assistance, contact McAfee technical support or your local authorized agent. Refer to “McAfee Support” in Chapter 1, “Introducing VirusScan NT.”