

---

# Installation and Setup

## Introduction

Even if you are a personal computer "power user" or are familiar with other anti-virus products, use the VirusScan NT installation procedure and follow the tasks outlined in this chapter. We are serious about this. Installing and running VirusScan NT is not like using other software.

The procedures must be followed in order to avoid spreading a computer virus infection. Viruses spread when you start your computer (sometimes called booting) from an infected hard disk or diskette, or when you run an infected program. If your computer is infected, installing and running VirusScan NT on your hard disk may spread the infection, even to the VirusScan programs themselves. The tasks in this chapter will ensure that you have a clean environment to detect, eradicate and prevent viruses.

By following these procedures you will be creating a virus-free environment, much like a surgical team establishing a "sterile field" before performing surgery. Once it is established, they make sure that everything brought into the field has already been sterilized. In this procedure, you will create a clean anti-viral start-up diskette with which you can always re-establish the sterile field.

Your VirusScan NT diskette is write-protected to ensure that no virus can alter the programs and information stored there.

 *Under no circumstances should you remove the write protection.*

## Overview

This chapter contains key information about installing VirusScan NT and creating a virus-free working environment. It is critical that you follow the installation and set up procedures outlined below. Using another method to install VirusScan NT could spread a virus, or even infect the VirusScan files themselves.

In this chapter, you will:

Step	Action
1.	Validate any VirusScan files obtained from a source other than McAfee.
2.	Install VirusScan NT, which encompasses: <ul style="list-style-type: none"><li>■ Scanning your system.</li><li>■ Modifying your setup files if needed.</li></ul>
3.	Make a clean DOS start-up diskette.
4.	Back up your hard disk.
5.	Rescan when you use new applications or diskettes.
6.	Update VirusScan regularly.

## System requirements

VirusScan NT requires an IBM-compatible personal computer, Windows NT, and a write-protected system diskette containing MS-DOS.

You will need a high-density 3.5" diskette drive to use the VirusScan install diskette in this package. Contact McAfee for other media, or download the software from the McAfee bulletin board system (BBS). Refer to ["McAfee Support"](#) in [Chapter 1, "Introducing VirusScan NT."](#)

If you download VirusScan NT from the McAfee BBS, we recommend that you also download Scan, a version of VirusScan for DOS. Scan can be used to remove viruses that infect the Master Boot Record or Boot Sector.

## Validate VirusScan

This task explains how to validate your VirusScan NT program files to ensure that you are installing software which has not been tampered with.

If you obtained VirusScan NT or one of its program files from any source other than the McAfee bulletin board or other McAfee service, it is important to verify that it is authentic, unaltered and uninfected. The VirusScan package includes the program, `Validate`, that will help you do this.

Use the following procedure to run `Validate` on the VirusScan program files:

Step	Action
1.	Launch a Windows 32-Bit Dos Command prompt to display the DOS prompt (C:\).
2.	Navigate to the directory to which you have downloaded or copied the files to. For example, if you have the files stored in C:\MCAFEE\VSCAN, type  <code>CD \MCAFEE\VSCAN</code>
3.	Type the command:  <code>validate ntscan.exe</code>

Compare the results with the information provided in the `PACKING.LST` file. If the validation results match what is in the file, it is highly unlikely that the program has been modified.

 *If the information in the text file does not match the results of the `Validate` program, or if you are at all unsure about the authenticity of any VirusScan file, contact McAfee for assistance. Refer to “McAfee Support” in Chapter 1, “Introducing VirusScan NT.”*

## Installing VirusScan NT

This task explains how to check your system and install the VirusScan NT software in the Windows NT environment.

 *Do not use any other method to install VirusScan NT, or you risk spreading a virus.*

### About installation

The VirusScan NT installation program performs certain tasks automatically: it scans your system, installs VirusScan NT and modifies your setup files (if needed). These tasks are described in detail later in this chapter.

The default installation destination is C:\MCAFEE\VIRUSCAN.

During installation, if the Install program finds any previously installed VirusScan files, it will ask whether to update them. If at any time you wish to leave the Install program, press [ESC] and you will return to Windows NT.

 *Be sure that no other anti-virus program is currently running before beginning the install, or the installation may fail.*

### Installation procedure

Follow the procedures as outlined below to install VirusScan on your system. Exit or unload any anti-virus programs before beginning the install process, or the installation may fail.

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

Step	Action
1.	Launch a Windows 32-Bit Dos Command Prompt to display the DOS prompt (C:).
2.	Insert the VirusScan program diskette in drive A.

3. Change to the A: drive by typing:

a :

4. Start the Install program by typing:

**install**

 *It may take several minutes for VirusScan program to check for viruses in memory, then on the system and user portions of your drives. VirusScan keeps you informed of its progress. Read the information carefully.*

5. If VirusScan continues with the installation after scanning, congratulations — most likely your system is currently virus-free. Follow the instructions on screen and, when finished, continue with [“Creating a clean DOS start-up diskette” on page 21](#).

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

```
Found the Jerusalem Virus in memory
```

**STOP THE INSTALLATION.** 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. *Go directly to [“If install detects a virus” on page 27](#) for details on how to remove the virus before you continue with the installation.*

 *VirusScan may report a “false alarm” if another anti-virus program is currently running. Ensure that all other anti-virus programs have been unloaded from memory before beginning the installation procedure. For more information, refer to [“False alarms” in Chapter 5, “Tips and Troubleshooting.”](#)*

6. Assuming Install did not find a virus, you will now be prompted to choose a directory for the VirusScan programs. We recommend that you choose the default, C:\MCAFFEE\VIRUSCAN. The files will be copied to this destination or to the destination you choose.

7. After you have successfully installed VirusScan NT, shutdown and restart your computer (in Program Manager, select File | Shutdown).
8. After restarting, you will make a clean DOS start-up diskette containing the Scan program for use in emergencies. Refer to “Creating a Clean DOS Start-Up Diskette” later in this chapter for instructions. **Be sure to write-protect the new diskette.**

Continue with this chapter to see how you can use VirusScan to keep your computer virus-free. We recommend that you also read [Chapter 3, “Using VirusScan NT,”](#) for information about using VirusScan NT to detect and remove viruses.

## Back up your hard disk

 *Ensure that your system is completely virus free before beginning this procedure. Perform this task immediately after you have completed a successful scan.*

Some viruses may leave certain disks or files unusable even after being “cleaned.” To avoid losing valuable data, back up your system regularly so you can restore your work should a virus destroy or damage important files. You should regularly scan your hard drive(s) and, if no viruses are detected, back up your files to fresh diskettes or backup tapes. You can use a commercial backup program or the one included with your operating system, but be sure to scan the backup program disk first to make sure that the backup program itself is not infected. Do not run the backup program if it is infected. Instead, reload it from your original installation diskettes.

## Creating a clean DOS start-up diskette

 *Ensure that your system is completely virus free before starting this procedure. Perform this task immediately after you have completed a successful scan.*

You should create a clean anti-viral DOS start-up (boot) diskette so that you can regain the “sterile field” should a boot sector infection occur. If you downloaded DOS Scan from the McAfee BBS, you will have to perform this procedure to create a DOS diskette containing Scan.

Step	Action
1.	Insert a diskette containing the MS-DOS system and then shutdown and restart your computer (in Program Manager, select File   Shutdown). The DOS prompt (A:\) should be displayed.

2.	Insert a blank or dispensable diskette in drive B. Make sure the diskette contains no important information, as this procedure will erase it.
----	---

3.	Format it as a start-up diskette with the system files by typing:
----	---

```
format b: /s/v/u
```

When prompted for a volume label, enter `virusfree01` or another name of up to 11 characters.

4.	If you downloaded VirusScan NT from the McAfee BBS, copy the Scan program files to the diskette, as shown in the following example:
----	---

```
copy c:\mcafee\viruscan\scan.exe b:
```

```
copy c:\mcafee\viruscan\scan.dat b:
```

```
copy c:\mcafee\viruscan\clean.dat b:
```

```
copy c:\mcafee\viruscan\names.dat b:
```

 *If you changed the default directory during installation your path will be different.*

5. You might also want to copy useful DOS programs to the diskette, as shown in the following example:

```
copy c:\dos\chkdsk.* b:
```

```
copy c:\dos\debug.* b:
```

```
copy c:\dos\diskcopy.* b:
```

```
copy c:\dos\fdisk.* b:
```

```
copy c:\dos\format.* b:
```

```
copy c:\dos\label.* b:
```

```
copy c:\dos\mem.* b:
```

```
copy c:\dos\sys.* b:
```

```
copy c:\dos\unerase.* b:
```

```
copy c:\dos\xcopy.* b:
```

In the same way, copy other DOS programs that you think might be useful.

 *If you use a disk compression utility, be sure to copy the drivers required to access the compressed disks onto the clean start-up diskette.*

6. Remove the diskette from the drive and write-protect it so that it cannot become infected.
- 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.
7. Label the diskette "Virus-Free Start-Up" and put it away in a secure place in case you need to reestablish a virus-free environment in the future. You may want to note the date and versions of DOS and VirusScan on the label.

---

## Rescanning new disks and software

McAfee recommends that you scan your disks when introducing new programs, or using disks that may be infected. New programs and files are generally introduced in two ways: by inserting a diskette and booting from it, and by installing new programs. It is also possible to download a virus via a modem.

For instructions on running VirusScan, refer to [Chapter 3, "Using VirusScan NT."](#)

---

### When you insert an unchecked diskette

Every time you insert a new diskette in your drive, run Scan on it before executing, installing or copying its files. If you have several diskettes to scan, you can scan them consecutively using the /MANY option described in [Chapter 3, "Using VirusScan NT."](#) In fact, McAfee recommends that you do this now with all the diskettes you normally use, as well as diskettes received from friends, co-workers, salespeople and even your own diskettes if they have been in another workstation.

---

### When you install or download 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 Scan on the directory in which the files were placed before you execute the files.

## Update VirusScan regularly

New viruses (and variants of old ones) appear and circulate often in the personal computer community. Fortunately, McAfee updates the VirusScan programs regularly — usually monthly, but sooner if many new viruses have appeared. Each new version can detect and remove as many as 60 to 100 new viruses or more, and can add new features. To find out what is new, review the README.1ST text file.

### Download new versions

You can download evaluation copies of new versions of McAfee products from the McAfee bulletin board. For more information, refer to “[McAfee Support](#)” in [Chapter 1, “Installation and Setup.”](#)

New versions of McAfee software are stored in compressed form to reduce transmission time.

 *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 still have the previously installed files.*

### Validate VirusScan

When you download a program file from any source other than the McAfee bulletin board 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 VirusScan, run Validate on all of the program files.

1. Launch a Windows 32-Bit Dos Command Prompt to display the DOS prompt (C:\).
2. Navigate to the directory to which you have downloaded the files. For example, if you have stored the files in C:\MCAFEE\DOWNLD\VIRUS-CAN:

```
cd \mcafee\downld\viruscan
```

3. Type the command:

```
validate ntscan.exe
```

```
validate scan.exe
```

4. Compare the results with the information in the PACKING.LST, README.1ST or other text 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.

## Update VirusScan

Once you have validated the new version, copy it into your C:\MCAFFEE\VIRUSCAN directory. In addition, you need to create a new start-up diskette or copy the Scan program files onto your existing clean start-up diskette.

### Updating VirusScan on your hard drive

Step	Action
1.	Launch a Windows 32-Bit Dos Command Prompt to display the DOS prompt (C:).
2.	Navigate to the directory to which you have retrieved the files, such as C:\MCAFFEE\DOWNLD\VIRUSCAN:  <pre>cd \mcafee\downld\viruscan</pre>
3.	Copy the contents of the directory to C:\MCAFFEE\VIRUSCAN:  <pre>copy *.* c:\mcafee\viruscan</pre>
4.	Shutdown and restart your computer (in Program Manager, select File   Shutdown   Shutdown and Restart) before performing any scans. VirusScan may report a “failed integrity check” if you attempt a scan immediately after an update.

## Updating your DOS start-up diskette

Follow the procedure outlined in “Make a Clean DOS Start-Up Diskette” to create an updated start-up diskette. Indicate the date, DOS version and VirusScan version on the new diskette. Store your older start-up diskette in a safe place to serve as a back-up.

If you want to upgrade your existing start-up diskette instead of creating a new one, use the following procedure:

Step	Action
1.	Temporarily remove write-protection from your clean DOS start-up diskette and insert it in drive A. <ul style="list-style-type: none"><li>■ For a 3.5” diskette, slide its corner tab so that the square hole is closed.</li><li>■ For a 5.25” diskette, remove the tab from its corner notch.</li></ul>
2.	Launch a Windows 32-Bit Dos Command Prompt to display the DOS prompt (C:).
3.	Copy the Scan program files to the diskette.  <code>copy c:\mcafee\viruscan\scan.exe a:</code>  <code>copy c:\mcafee\viruscan\scan.dat a:</code>  <code>copy c:\mcafee\viruscan\clean.dat a:</code>  <code>copy c:\mcafee\viruscan\names.dat a:</code>
4.	Remove the diskette from the drive and write-protect it again.

## If install detects a virus

VirusScan's installation procedure begins with a scan of your computer's memory and all local drives (including hard drives, compressed, CD-ROM and PCMCIA drives, but not diskettes). If a virus is detected, a message similar to the following is displayed:

```
Scanning C:  
  
Scanning file C:\DOS\ATTRIB.EXE  
  
Found the Jerusalem Virus
```

Stop the installation. **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. Follow the steps outlined below to use DOS Scan to eliminate the virus and clean or delete any infected files before continuing with the installation.

 *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 will also use DOS Scan to remove a Master Boot Record (MBR) or Boot Sector virus. **Do not attempt to remove Master Boot Record (MBR) or Boot Sector viruses using NTScan.** These viruses can be removed using DOS Scan by following the procedures below.

### 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 “Create a Clean DOS Start-Up Diskette” earlier in this chapter, but only *after* you have successfully cleaned your system.)

Step	Action
1.	Shutdown your computer (in Program Manager, select File   Shutdown). (Do not just reset or reboot, since doing so 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,” below.
- If Scan reports that the virus could not be safely removed, refer “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” on page 17. 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 “Rescanning new disks and software” on page 23.

### 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.” If you have any questions, contact McAfee (refer to “McAfee Support” in Chapter 1, “Introducing VirusScan NT”).

After the virus-infected files are deleted, begin the installation procedure again as described in “Installing VirusScan NT” on page 17. 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 “Rescanning new disks and software” on page 23.

