Multi-Platform Quick Start Guide

Command AntiVirus™
with CSS Central Administration

For Windows® 95, DOS, Windows®,
Windows NT® Workstation,
Windows NT® Server, and NetWare®

NOTICE

Command Software Systems, Inc. (CSSI) reserves the right to make improvements in the product described in this manual at any time and without prior notice.

This material contains the valuable properties and trade secrets of CSSI, a Florida corporation, embodying substantial creative efforts and confidential information, ideas and expressions, no part of which may be reproduced or transmitted in any form or by any means, electronic, mechanical, or otherwise, including photocopying, and recording, or in connection with any information storage or retrieval system, without prior written permission from CSSI.

LICENSE AGREEMENT

This software package is protected by United States copyright laws and international copyright treaties, as well as other intellectual property laws and international treaties.

1. **License Grants.** Licensor hereby grants Licensee the right to use, as set forth below, the number of copies of each version number and language of Software set forth on the cover page of the License Agreement.

a. **Application Products** – **For products which are classified in the Open License Estimated Retail Price List as belonging to the Application Product Pool, the following applies:**

(I)For application products not otherwise identified below, the following section is applicable

For each License acquired, Licensee may use one copy of the Software, or in its place, any prior version for the same operating system, on a single computer.

Licensee may also store or install a copy of the Software on a storage device, such as a network server, used only to install or run the Software on Licensee's other computers over an internal network; however, Licensee must acquire and dedicate a License for each separate computer on which the Software is installed or run from the storage device. A license for the Software may not be shared or used concurrently on different computers.

Licensee must retain this License Agreement as evidence of the license rights granted by Licensor. By executing the rights granted to Licensee in this License Agreement, Licensee agrees to be bound by its terms and conditions. If Licensee does not agree to the terms of this License Agreement, Licensee should promptly return it together with all accompanying materials and documents for a refund.

WARRANTY

CSSI warrants the physical diskette and the physical documentation to be free of defects with respect to materials and workmanship for a period of thirty days from the date of purchase. During the warranty period, CSSI will replace the defective disk or documentation. This warranty is limited to replacement and does not encompass any other damages. CSSI MAKES NO OTHER EXPRESS OR IMPLIED WARRANTIES ON THE SOFTWARE INCLUDING THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE AND THE WARRANTY OF MERCHANTABILITY.

Document No. MQS-454-1098

Part No. 07-9001-00

Table of Contents

INTRODUCTION

Congratulations on choosing Command AntiVirus for unsurpassed security against viruses! You do not have to be an experienced computer user to take full advantage of the protection offered. Command AntiVirus safely removes viruses from documents, boot sectors and partition tables. This superior virus detection and disinfection is provided by the F-PROT Professional engine.

Command AntiVirus real-time protection provides continuous background scanning in Windows, Windows 95, Windows NT and NetWare. This additional layer of defense keeps your systems safe between scans.

CSS Central provides system administrators with an easy-to-use interface for distributing, updating and modifying Command AntiVirus from a central location. CSS Central can be run on Windows NT server and workstation version 4.0 and above and on Windows 95.

NOTE: CSS Central can be installed as part of Command AntiVirus for Windows NT Server. It is also available as a separate product. CSS Central is for use by System Administrators and/or experienced users of Command Software Systems' products.

The Multi-Platform Quick Start provides a brief overview of our products and basic start up instructions. You can find detailed information in the platform-specific manuals. These manuals are included on the Command AntiVirus CD and are available for download from our web site at **www.commandcom.com**.

MAIN FEATURES

Command AntiVirus (CSAV) is a comprehensive virus protection program that:

- Uses state-of-the-art technology to scan for thousands of known viruses and their variants.
- Prevents infected programs from running.
- Has ICSA certification for effective virus protection.

- Removes viruses without damaging the original file.
- Scans for boot sector viruses, macro viruses, and Trojan Horses.
- Scans hard drives, diskettes, CD-ROMs, network drives, directories, and specific files.
- Scans PKZIP-compressed files and compressed executables including PKLITE, DIET and ICE-PACK.
- In Windows NT and 95 provides right mouse button support which allows you to easily start a scan on any file or folder.
- In Windows NT provides a service which allows scheduled scans to run in the background on both local and network drives.
- Provides complete scan scheduling which allows you to assign scans to a specific day, week, month or after periods of inactivity. (Not available for DOS & Windows.)
- Provides fully configurable inclusion and exclusion of files and folders from the scan list.
- Provides enterprise-wide messaging capabilities including electronic mail.
- Provides a comprehensive virus database which allows you to identify the type and origin of virus infection.
- Provides companion product notification with Command AntiVirus for NetWare.

TESTING COMMAND ANTIVIRUS

For testing purposes, there is a self-extracting file called SE_EICAR.EXE provided on the distribution diskettes. If you run this file, you will find a test file called EICAR.COM (from the European Institute for Computer Anti-Virus Research). This file helps you verify that you installed your anti-virus protection properly and that DVP on-access protection is working. EICAR.COM lets you safely test custom messages that you create, and it also provides a way to demonstrate what happens when a virus is found.

To test the Command AntiVirus scanner, you can either copy EICAR.COM to your hard drive and run a scan or you can leave it on a diskette and then scan that diskette. To test the on-access protection of DVP in Windows 3.1x, Windows 95 and Windows NT, run or copy the file.

If DVP is **not** active when you run EICAR.COM, the system displays the following message:

```
"EICAR-STANDARD-ANTIVIRUS-TEST-FILE!"
```

If DVP **is** active when you run EICAR.COM, the system displays the following message:

```
DVP FOR WINDOWS NT: VIRUS DETECTED
A:\ EICAR.COM INFECTION: EICAR_TEST_FILE
```

TESTING ON NETWARE

EICAR.COM lets you safely test the notification capabilities of AlertTrack™. It also provides a way to demonstrate what happens when a virus is found, in addition to testing the on-access protection.

To test on-access protection during **Scan on Opens**, copy EICAR.COM to a test directory on the server and try to run the file.

To test on-access protection during **Scan on Closes**, copy EICAR.COM to a test directory on the server. The file is placed in a queue, and the scan is executed at the end of a specified time (the default is 5 minutes). You can change this "closed scan delay" by typing the following command prior to copying the file:

```
F-PROT C(LOSE) S(CAN) D(ELAY) = {SECONDS OR MM:SS}
```

If on-access protection **is** active, a message similar to the following one will be displayed in the areas that you have selected. By default, infected files go to the Command AntiVirus screen and the Command AntiVirus log file.

```
04/26/96  16:56:08:
SYS:TEST\ EICAR.COM INFECTION: EICAR_TEST_FILE
```

ADDITIONAL INFORMATION

WEB SITE

You will find a wealth of fascinating information on the Command Software Systems web site. Do you have questions about viruses? Do you want to know more about security? Would you like to view the answers to our customers' most frequently asked questions? We provide comprehensive information on viruses, products, events, employment opportunities and much more. Plus, for your convenience, all of our readme files, quick start guides, and manuals are available for online viewing.

Be sure to visit this exciting extension of Command Software Systems' services at **www.commandcom.com** or our web site in the UK at **www.command.co.uk**.

HELP FILES

The Help files for each platform contain additional information and include links to our web site where you can view the manuals online.

MAILING LIST SERVER

Registered users of Command AntiVirus can subscribe to Command Software Systems' mailing list server. As long as you have an Internet e-mail address, you can obtain electronic notification of product updates and announcements. You can also receive our newsletter and a variety of other services. For more information, call Customer Service or visit our web site.

README.TXT

The latest information on product enhancements, bug fixes and special instructions are in the README.TXT file. If you like, you can review this file, prior to download, on the Command Software Systems web site.

CSAV FOR WINDOWS 95

SYSTEM REQUIREMENTS

To operate Command AntiVirus for Windows 95, you must have Microsoft Windows 95 installed on an IBM-compatible computer with at least 8MB of RAM and 4MB of available hard-disk space.

INSTALLATION

The following instructions allow you to install Command AntiVirus for Windows 95 quickly and easily using the default options.

QUICK INSTALL

NOTE: We strongly recommend that you exit all Windows programs before running the setup program.

1. Insert the CD-ROM.
2. Click the **Start** button.
3. Click **Run**.
4. Select **Browse** to search the CD for the **WIN95** directory.
5. Change to that directory.
6. Double-click **SETUP.EXE** and click **OK**.
7. After startup, the system displays the Welcome screen. Click **Next**.
8. Select **Default** from the **Setup configuration** screen. Command AntiVirus for Windows begins the installation process.
9. Follow the instructions on the screen.

After installation, you can access Command AntiVirus by double-clicking the yellow **C** icon found in the tray on the right side of the taskbar. Or, you can create a permanent shortcut as described next.

NOTE: If you are using diskettes, insert Disk #1 into drive A. After you have completed Steps 2 and 3, type **A:\setup** and press **Enter**. To complete the installation, continue to Step 7.

During the installation, the system prompts you for the additional diskettes.

CREATING A SHORTCUT

There are many ways to create shortcuts for easy access to Command AntiVirus. The following is one example:

1. Right click the desktop.
2. Click **New**.
3. Click **Shortcut**.
4. Select **Browse**.
5. Double-click **Program Files**.
6. Double-click **Command Software**.
7. Double-click **F-PROT95**.
8. Select **F-PROT32.EXE** and then **Open**.
9. Select **Next** and then **Finish**.

CREATING A RESCUE DISK

If you did not choose to make a Command AntiVirus rescue disk during installation, you can run the setup program again and one will be created automatically. You can also can create one manually. Make sure that your system is **virus-free** before beginning this task.

If you prefer to make a Command AntiVirus rescue disk manually, refer to the **Installation** chapter in the *Command Anti-Virus for Windows 95 User's Guide*.

SCANNING FEATURES

Command AntiVirus for Windows 95 contains the following scanning features.

SCHEDULED SCANS

You can schedule a scan for a specific day, week or month. You can specify the time you want the scan to occur, or you can schedule a scan to run after a specified time of inactivity. To create a daily scheduled scan of your hard drive, select **Scan Hard Drives** and then click the **Properties** button. From the **Properties** dialog box, click the **Schedule** button and be sure that the **Enable Scheduling** option has a check mark in it. Specify the time of day in 24-hour format with 00:00 indicating midnight. If the computer is **not** on during the specified time, the scheduled scan is skipped.

MANUAL SCANS

After installation, start the scan by clicking the desired task name and then clicking the **Execute Task** button. This starts a scan that, by default, gives a report if a virus is found. Should a virus be found, disinfection will not occur until the action to take is modified. This can be done by selecting a task name, clicking the **Properties** button, and then selecting the **Action to take** pull-down menu.

CUSTOM SCANS

Command AntiVirus for Windows 95 comes configured with standard scanning tasks. You can create your own custom scan quickly and easily by clicking the **New Task** button and naming the task. The system displays the **Properties** dialog box. From here, you can select the action to take, the drive/path to scan, and files to scan. You can also set up a schedule.

DYNAMIC VIRUS PROTECTION

Dynamic Virus Protection (DVP) provides on-access protection against viruses by scanning the boot sector every time a diskette is read and by scanning every program file prior to execution. From the **Preferences**/**Active Protection** menu, you can enable or disable DVP and select whether to scan diskette drives, local hard drives or network drives. You can also select the action to take on infection.

MEMORY SCANNING

Memory scanning is available by selecting **Active Protection** from the **Preferences** menu. Click the Memory Scanning tab and select or clear the memory scanning check box to make the function active or inactive.

AUTOMATIC UPDATE

This option allows system administrators to automatically perform partial or full-product updates of Command AntiVirus on each workstation when the user starts the computer. **Automatic Update** also allows each user to manually update a workstation. For more information, refer to **Automatic Update** located in the ***Network Administration*** chapter.

REMOVING COMMAND ANTIVIRUS

If you want to remove Command AntiVirus for Windows 95, follow these directions:

1. Double-click **My Computer**.
2. Double-click **Control Panel**.
3. Double-click **Add/Remove Programs**.
4. Click **Command AntiVirus for Windows 95**.
5. Click **Remove**.
6. Follow the default suggestions on the screen.

CSAV FOR DOS

SYSTEM REQUIREMENTS

To operate Command AntiVirus for DOS, you must have DOS 3.3 or higher installed on an IBM-compatible 80386 computer with at least 640K of RAM and 1.5MB of available hard-disk space.

You can use Command AntiVirus on a workstation connected to a Windows NT®, NetWare®, 3Com© or Banyan® Vines® network.

INSTALLATION

This product comes with a DOS **INSTALL** program.

During the installation, the program does the following:

- Creates a directory and copies the Command AntiVirus files to it.
- Offers to modify your AUTOEXEC.BAT in order to provide a daily scan of the hard drive.

For quick installation, simply accept the default options.

To insure that your system is **virus-free**, we recommend that you run the DOS scanner from Command AntiVirus Installation Disk #2 before installing the product. To begin the scan:

1. Insert Command AntiVirus Disk #2 into drive A.
2. At the command line, type **A:**
3. Press **Enter**.
4. When the system displays the A: prompt, type **CD**
5. Press **Enter**.
6. Type **F-PROT /HARD**
7. Press **Enter**. The program scans all physical hard drives.

If the system reports a virus prior to or during installation, you **must** disinfect the drive before continuing. For more information, refer to **If a Virus is Found** located in the *Command AntiVirus for DOS User's Guide*.

INSTALLING

To begin the installation process, complete the following steps:

1. Insert Command AntiVirus Disk #1 into drive A.
2. At the DOS command line, type **A:\INSTALL**
3. Press **Enter**. The system displays the **Welcome** screen.
4. Press **Enter** to continue. The system displays the **Main Menu** screen.
5. Follow the default selections on the screen.

NOTE: If you are using a CD, insert the CD-ROM. Search the CD for the **DOS** directory, and change to that directory. Type **INSTALL**. To complete the installation, continue to Step 3.

CREATING A RESCUE DISK

The following instructions will help you create a rescue disk. A rescue disk allows you to start your system in DOS and then run Command AntiVirus from the diskette. Make sure that you have a blank high-density diskette on hand and that the diskette and your system are **virus-free**.

1. At the DOS command line, change to the F-PROT directory and type:
   RESCUE
2. Press **Enter**.
3. Insert a diskette into drive A.
4. Press **Enter**. The system displays a warning that the diskette will be formatted.
5. Press **Enter**. The system prompts you to insert a diskette.
6. Press **Enter**. The system formats the diskette. When the formatting is complete, the system asks if you would like to format another diskette.
7. Type **N**.
8. Press **Enter**. The system begins copying the files.
9. When the system has finished copying, remove the diskette from drive A.

10. Label this diskette “Command AntiVirus Rescue Diskette For (Users Computer ID).”
11. Set the write-protect tab to prevent any modifications to the diskette.

Because the rescue file is machine-specific, the diskette is only for the computer used to create the file. If you want to modify the rescue disk, create it manually. See **Creating a Rescue Disk** in the *Command AntiVirus for DOS User’s Guide*.

TESTING THE RESCUE DISK

Test your rescue disk by performing the following steps:

1. Turn off your computer for about 15 seconds.
2. Insert the Rescue Disk into Drive A.
3. Turn on your computer. After startup, the system notifies you that Command AntiVirus will scan your hard drive for viruses.
4. Press **Enter**.
5. When the scanning is complete, remove the diskette from drive A.

NOTE: If you are using a Rescue Disk that you created manually, the system does not scan automatically. After system startup when the A: prompt appears, type:

```
F-PROT /HARD /DISINF
```

You have just created and tested a rescue boot disk. Put the diskette in a safe place until you get your next Command AntiVirus update. Hopefully, you will never have a need for it.

SCANNING FEATURES

Command AntiVirus for DOS contains the following scanning features.

AUTOMATED SCANS

The default installation places the following statement in the AUTOEXEC.BAT file:

```
C:\F-PROT\F-PROT /HARD /TODAY
```

This statement starts a daily scan of memory and the local hard drives when you start your computer for the first time on any given day.

MANUAL SCANS

After installation, you can perform a manual scan by completing the following steps:

1. Type **CD\F-PROT**.
2. Press **Enter**.
3. Type **F-PROT**.
4. Press **Enter**. F-PROT.EXE performs a scan for any viruses that may be in memory. When the program completes the memory check, the system displays the **Main** menu.
5. Select **Begin Scan**.
6. Press **Enter**.

Before selecting **Begin Scan**, you can specify how you want your scan to operate. Using the default settings, the program scans your hard drive to check executable files and then generates a report.

MEMORY SCANNING

The program automatically scans memory.

REMOVING COMMAND ANTIVIRUS

If you want to remove a default installation of Command AntiVirus for DOS, perform the following steps manually:

1. Delete all files from C:\F-PROT and remove the directory.
2. Remove the C:\F-PROT directory from the SET PATH= statement in the AUTOEXEC.BAT.
3. Delete the following line from the AUTOEXEC.BAT:

```
\F-PROT\F-PROT /HARD /TODAY
```

CSAV FOR WINDOWS

SYSTEM REQUIREMENTS

To operate Command AntiVirus for Windows, you must have Windows 3.1 or higher or Windows for Workgroups 3.11 installed on an IBM-compatible computer with a least 4MB of RAM and 4MB of available hard-disk space.

You can use Command AntiVirus on a workstation connected to a Windows NT®, NetWare®, 3Com© or Banyan® Vines® network.

INSTALLATION

This product comes with a Windows **SETUP** program that allows you to install all of the necessary files to protect your system in the Windows environment. You can also choose to install CSAV For DOS.

During the installation, the program does the following:

- Creates a directory and copies the Command AntiVirus files to it.
- Installs on-access scanning.
- Gives you the option to install CSAV For DOS.
- Gives you the option to modify your AUTOEXEC.BAT to provide a daily scan of the hard drive if you have chosen to install CSAV For DOS.

To insure that your system is **virus-free**, we recommend that you run the DOS scanner before installing the product. To begin the scan:

1. Insert the CD-ROM.
2. At the command line, type **X:** The letter X represents the letter of your CD-ROM drive.
3. Press **Enter**.
4. When the system displays the X: prompt, type **CD\DOS**

5. Press **Enter**.
6. Type **F-PROT /HARD**
7. Press **Enter**. The program scans all physical hard drives.

If the system reports a virus prior to or during installation, you **must** disinfect the drive before continuing. For more information, refer to **If a Virus is Found** located in the *Command AntiVirus for Windows User's Guide*.

NOTE: If you are using diskettes, you **must** insert Command AntiVirus for DOS Installation Disk #2 into drive A. Remember to substitute drive letter A for the letter X. After you have completed Steps 2 and 3, type **CD**. To complete the installation, continue to Step 5.

INSTALLING

NOTE: Do not run a DOS shell under Windows to install.

To begin the installation process, complete the following steps:

1. Insert the CD ROM.
2. From the menu bar at the top of the Program Manager, click **File** and then **Run**. The system displays the Run dialog box.
3. Select **Browse** to search the CD for the **WIN31** directory.
4. Change to that directory.
5. Double-click **SETUP.EXE** and click **OK**.
6. After startup, the system displays the Welcome screen. Click **Continue**.
7. The system displays the Command AntiVirus Setup dialog box. Follow the default selections on the screen.

NOTE: If you are using diskettes, insert Disk #1 into drive A. After you have completed Step 2, type **A:\setup** and press **Enter**. To complete the installation, continue to Step 6.

During the installation, the system prompts you for the additional diskettes. To install CSAV for DOS, you **must** have Command AntiVirus for DOS Disk #2.

CREATING A RESCUE DISK

NOTE: You **must** have CSAV for DOS installed to create a rescue disk.

The following instructions will help you create a rescue disk. A rescue disk allows you to start your system in DOS and then run Command AntiVirus from the diskette.

Make sure that you have a blank high-density diskette on hand and that the diskette and your system are **virus-free**.

1. In Windows, select **File/Run** and type:

   ```
   \F-PROT\RESCUE
   ```

2. Press **Enter**.
3. Insert a diskette into drive A.
4. Press **Enter**. The system displays a warning that the diskette will be formatted.
5. Press **Enter**. The system prompts you to insert a diskette.
6. Press **Enter**. The system formats the diskette. When the formatting is complete, the system asks if you would like to format another diskette.
7. Type **N**.
8. Press **Enter**. The system begins copying the files.
9. When the system has finished copying the files, remove the diskette from drive A.
10. Label this diskette "Command AntiVirus Rescue Diskette For (Users Computer ID)."
11. Set the write-protect tab to prevent any modifications to the diskette.

Because the rescue file on the diskette is machine-specific, this diskette is only for the computer used to create the file.

If you want to modify the rescue disk, you can create the rescue disk manually. For more information, refer to **Creating a Rescue Disk** in the *Command AntiVirus for Windows User's Guide*.

TESTING THE RESCUE DISK

Test your rescue disk by performing the following steps:

1. Turn off your computer for about 15 seconds.
2. Insert the Rescue Disk in Drive A.
3. Turn on your computer. After startup, the system notifies you that Command AntiVirus will scan your hard drive for viruses.
4. Press **Enter**.
5. When the scanning is complete, remove the diskette from drive A.

NOTE: If you are using a Rescue Disk that you created manually, the system does not scan automatically. After system startup when the A: prompt appears, type:

```
F-PROT /HARD /DISINF
```

You have just created and tested a rescue boot disk. Put the diskette in a safe place until you get your next Command AntiVirus update. Hopefully, you will never have a need for it.

SCANNING FEATURES

Command AntiVirus for Windows contains the following scanning features.

AUTOMATED SCANS

The default installation places the following statement in the AUTOEXEC.BAT file:

```
C:\F-PROT\F-PROT /HARD /TODAY
```

This statement starts a daily DOS-based scan of memory and the local hard drives when you start your computer for the first time on any given day.

Scan On Load

In Windows, the **Scan on Load** option allows you to perform a scan automatically each time you run Command AntiVirus from Windows. Select **Scan on Load** from the **Options** menu.

Selecting this item places a check mark next to the item. Selecting the item again clears the check mark. Once you have selected the item, you must save

your settings in a configuration file, for example, DEFAULT.FPW. For more information, refer to **File Menu** located in the C*ommand AntiVirus for Windows User's Guide*.

Now, when you double-click on the Command AntiVirus icon in the Command AntiVirus window, the program automatically begins a scan. If the program finds an infection, the summary dialog box appears.

NOTE: If you want a scan to run automatically every time you launch Windows, the Command AntiVirus icon **must** be copied to your Startup group. You can edit the properties of the icon to run the program minimized.

Scan once a day

If you do not automatically scan once a day when you first start your system, this option performs a full scan of memory and the hard drive the first time you enter Windows each day. For more information, refer to **Modifying AUTOEXEC.BAT** located in the C*ommand AntiVirus for Windows User's Guide*. **Scan once a day** is available by selecting **Advanced Options** from the **Options** menu and selecting **Scan once a day**.

For **Scan once a day** to work, you **must** copy the Command AntiVirus icon to your Startup group, select the **Scan on Load** option in the **Options** menu, and, if applicable, make changes to your AUTOEXEC.BAT. For more information, refer to **Scan on Load** located previously in this quick start guide.

Scan after inactivity of XX minutes

In Windows, this option provides a convenient method of scanning when the computer is not active. **Scan after inactivity of XX minutes** is available by selecting **Advanced Options** from the **Options** menu. Select **Scan after inactivity of XX minutes** and specify the number of minutes of inactivity (including keyboard and mouse) that should pass before the program begins the specified scan.

Command AntiVirus **must** be open or minimized for **Scan after inactivity of XX minutes** to work.

MANUAL SCANS

After installation, you can perform a manual scan by completing the following steps:

In Windows

1. At the Program Manager window, double-click the Command AntiVirus group icon. The system displays the Command AntiVirus window.
2. Double-click the Command AntiVirus icon. The system displays the **Scan Options View**.
3. Click **Begin Scan**.

In DOS

1. Type **CD\F-PROT**.
2. Press **Enter**.
3. Type **F-PROT**.
4. Press **Enter**. F-PROT.EXE performs a scan for any viruses that may be in memory. When the program completes the memory check, the system displays the **Main** menu.
5. Select **Begin Scan**.
6. Press **Enter**.

Before selecting **Begin Scan**, you can specify how you want your scan to operate. Using the default settings, the program scans your hard drive to check executable files and then generates a report.

MEMORY SCANNING

This option allows you to scan memory. We recommend scanning memory whenever you start your system.

In Windows, memory scanning is available by selecting **Active Protection** from the **Options** menu. Double-click **Memory Scanning** and select or clear the memory scanning check box to make the function active or inactive.

In DOS, the program automatically scans memory.

ON-ACCESS PROTECTION

On-access scanning, an important element of protection, prevents your system from becoming infected between full scans. This on-access protection is provided in Windows through Dynamic Virus Protection (DVP). DVP is a virtual device driver (VxD) for the Windows environment.

DVP provides transparent, real-time scans of each program run. This includes programs run from the hard drive, a diskette or CD-ROM, and the boot sector of each diskette that is read. The moment you place a diskette or CD-ROM in the drive and run or copy a program, the diskette or CD-ROM is automatically scanned. DVP also scans files that are opened in a DOS window, but does not scan files that are opened in DOS.

AUTOMATIC UPDATE

This option allows system administrators to automatically perform partial or full-product updates of Command AntiVirus on each workstation when the user starts the computer. **Automatic Update** also allows each user to manually update a workstation. For more information, refer to **Automatic Update** located in the ***Network Administration*** chapter.

REMOVING COMMAND ANTIVIRUS

If you want to remove a default installation of Command AntiVirus for Windows, perform the following steps manually:

1. Delete all files from C:\F-PROT and remove the directory.
2. Remove the C:\F-PROT directory from the SET PATH= statement in the AUTOEXEC.BAT.
3. If you selected the **Place CSAV DOS in AUTOEXEC.BAT** option, delete the following line:
   ```
   \F-PROT\F-PROT /HARD /TODAY
   ```
4. Delete the following components of the WIN.INI file in the Windows directory:
   ```
   RUN=C:\F-PROT\DVP31.EXE
   ```
5. Delete the following line from the SYSTEM.INI file:
   ```
   DEVICE=C:\F-PROT\DVP.VXD
   ```
6. Delete the DVP Preference section from the SYSTEM.INI file.

CSAV FOR NT WORKSTATION

SYSTEM REQUIREMENTS

To operate Command AntiVirus for NT Workstation, you must have Microsoft Windows NT® 3.51 or higher installed on an IBM-compatible 386/25 computer with at least 16MB of RAM and 4MB of available hard-disk space.

INSTALLATION

NOTE: We strongly recommend that you exit all Windows programs before running the setup program.

There are two sets of installation instructions: Standard Installation and Setup for Network Administrators. Choose the one that is best suited for your situation.

STANDARD INSTALLATION INSTRUCTIONS

To install Command AntiVirus, you must be logged on as a member of the local administrators group.

1. Insert the CD-ROM.
2. Click the **Start** button (NT 4.0) or select **Run** from the **File** menu of the Program Manager (NT 3.51).
3. Select **Browse** to search the CD for the **WINNT** directory.
4. Change to that directory.
5. Double-click **SETUP.EXE** and click **OK**.
6. Select either the **Default** or the **Custom** configuration. The **Default** installation allows workstation users to set up Command AntiVirus for NT Workstation on their local computers. **Custom** lets you select the components that you want installed.

7. If your computer is connected to a network, the next dialog box that appears is the **Service Account for Network Scans**. There is a check box at the bottom that says "I'd like to be able to schedule scans of network drives".

   By default, the box is selected. If you clear this check box, scanning of network drives will be limited to manual scans. If you clear the check box and click **Next**, the installation begins. If you do not clear the check box, a **Command Software AV Scheduling Service** dialog box opens.

8. In the **AV Scheduling Service** dialog box, the current user information is displayed by default. If you are using your current account, enter your current password. If you want to change the information, use an account that meets the following criteria:
   A. The Username must reflect an existing account.
   B. The account must have rights to access network drives.
   C. Scanning requires that the user has **Read** access. To disinfect, quarantine or delete, the user must have **Write** access.

NOTE: If possible, use a password that does not expire. If you change the password for this account, you must change it in Command AntiVirus (**Preferences|Advanced|Service Account**). If your password expires, scheduled scans will not function on network drives.

If you enter an account that does not exist or if you enter an invalid password, Command AntiVirus will not validate the service account. As a result, scans of network drives will not take place and Windows NT's Event Viewer will log a message regarding the invalidated service account.

Manual scans of local and network drives are allowed and DVP is active by default.

9. You are asked if you want to make a rescue disk. If so, insert a **virus-free** diskette into the diskette drive. Command AntiVirus formats the diskette and adds the necessary files.

NOTE: Select **No** when asked to format another diskette.

10. When SETUP is complete, the system displays the **Setup Complete** dialog box. Select **Finish** and you are done!

NOTE: If you are using diskettes, insert Disk #1 into drive A. After you have completed Steps 2 and 3, type **A:\setup** and press **Enter**. To complete the installation, continue to Step 7.

During the installation, the system prompts you for the additional diskettes.

SETUP FOR NETWORK ADMINISTRATORS

The **NETADMIN** parameter can be added to the command line when installing Command AntiVirus for NT Workstation. Using this command sets up an area on the network for users to install from so that individual CD's or diskettes are not needed for each workstation. Plus, by using the **NETADMIN** command, the System Administrator can control some key functions of Command AntiVirus.

Some of these functions include preventing users from turning off real-time protection, restricting users from manually scanning network drives, and disabling users' ability to disinfect viruses.

To use this capability, follow these steps:

1. Insert the CD-ROM.
2. Click the **Start** button (NT 4.0) or pull down the **File** menu of the Program Manager (NT 3.51).
3. Click **Run**.
4. Select **Browse** to search the CD for the **WINNT** directory.
5. Change to that directory.
6. Click **SETUP**. The system displays the Run dialog box containing the word SETUP.
7. Add a space and type **NETADMIN**.
8. Press **Enter**.
9. The system displays the Welcome screen and then the **Network Setup Configuration** dialog box.

   Enter the location on the network where you want to store the shared components of Command AntiVirus. Use a Universal Naming Convention (UNC) path that does not include spaces. This is necessary because InstallShield's SETUP.EXE is a 16-bit application and spaces included in a path will cause an error. The following is an example of a valid UNC path:

   ```
   \\SERVER\SHARED\INSTALL\SHARE
   ```

These files include F-PROT.EXE, the .FPT files (Command AntiVirus Task), Help files, the readme file, and assorted .DLL's.

10. Enter the location for the SETUP components. This is the area on the network that users will access so that they can install Command AntiVirus. Use a UNC path that does not include spaces. This is necessary because InstallShield's SETUP.EXE is 16-bit application and spaces included in a path will cause an error. The following is an example of a valid UNC path:

    ```
    \\SERVER\SHARED\INSTALL\SETUP
    ```

11. There is a check box that controls whether you want users to be able to scan network drives. Decide which is best for you. If you clear the check box, go to Step 14.
12. Select **Next**.
13. The next screen lets you enter information about the account that users will use for scheduled scans of network drives. Use an account that meets the following criteria:
    A. The Username must reflect an existing account.
    B. The account must have rights to access network drives.
    C. Scanning requires that the user has **Read** access. To disinfect, quarantine or delete the user must have **Write** access.
    D. The account should be accessible for all users.

NOTE: If possible, use a password that does not expire. If you change the password for this account, you must also update it in Command AntiVirus (**Preferences|Advanced|Service Account**). If the password expires, scheduled scans will not function on network drives.

14. Select **Next**. Setup begins.
15. The **Command AntiVirus Config** dialog box opens. Fill in your name and company information.
16. Select **Options** to view or modify Command AntiVirus capabilities. Select or clear the choices, then click **OK** to save your settings or click **Cancel**.
17. Setup continues and a final dialog box opens to confirm that the installation was successful.

In the setup components location you selected, there are four batch files. Two of them (CLIENT.BAT and SILENT.BAT) allow you to install Command AntiVirus from the setup location on the network using a shared location with only a few files residing on the local workstation. The other two batch files

(LCLIENT.BAT and LSILENT.BAT) let you install all components to the local workstation.

By running CLIENT.BAT from the workstation, all the components necessary to run Command AntiVirus are automatically installed with a minimum of user intervention. SILENT.BAT does the same installation, however, **no** user intervention is needed. The result is to have DVP (on-access protection) installed on the local workstation as well as having CSS AV Scheduler installed so that scheduled scans can occur.

LCLIENT.BAT or LSILENT.BAT function as described above except that all of the Command AntiVirus components are installed on the local workstation.

After installation, you can access Command AntiVirus by double-clicking the yellow **C** in the tray on the right side of the taskbar. Or, you can create a permanent shortcut as described next.

NOTE: If you are using diskettes, insert Disk #1 into drive A. After you have completed Steps 2 and 3, type **A:\SETUP NETADMIN**. To complete the installation, continue to Step 8.

During the installation, the system prompts you for the additional diskettes.

CREATING A SHORTCUT

If you are using Windows NT 4.0, you may want to create a shortcut for easy access to Command AntiVirus. There are many ways to create shortcuts. The following is one example:

1. Right click the **desktop**.
2. Click **New**.
3. Click **Shortcut**.
4. Select **Browse**.
5. Double-click **Program Files**.
6. Double-click **Command Software**.
7. Double-click **F-PROTNT**.
8. Select **F-PROT32.EXE** and then **Open**.
9. Select **Next** and then **Finish**.

In Windows NT 3.51, a program group containing the icons for Command AntiVirus will be created for your desktop.

CREATING A RESCUE DISK

If you did not create a Command AntiVirus rescue disk during installation, you can run the setup program again and one will be created automatically. You can also create one manually. Make sure that your system is **virus-free** before beginning this task.

If you prefer to make a Command AntiVirus rescue disk manually, refer to the **Installation** chapter in the *Command AntiVirus for NT Workstation User's Guide*.

SCANNING FEATURES

Command AntiVirus for NT Workstation contains the following scanning features.

SCHEDULED SCANS

Command AntiVirus for NT Workstation includes a service (CSS AV Scheduler) that runs scheduled and inactivity scans in the background. With this feature, the users' work flow is not interrupted while Command AntiVirus's protection operates invisibly behind the scenes.

A scan may be scheduled for a specific day, week or month. You can specify the time you want the scan to occur, or you can schedule a scan to run after a specified time of inactivity.

To create a daily scheduled scan of your hard drive, select **Scan Hard Drives** and then click the **Properties** button. From the **Properties** screen, click the **Schedule** button and be sure the **Enable Scheduling** option has a check mark in it. Specify the time of day in 24-hour format with 00:00 indicating midnight. If the computer is **not** on during the specified time, scheduled scans will be skipped.

QUICK SCANS

Within Command AntiVirus for NT Workstation, you can activate a shortcut menu that allows you to perform fast and efficient virus scans of selected folders or files. The files or folder to be scanned can be located in Windows NT's Explorer, on the desktop, or within program groups.

To perform a scan from the shortcut menu, select one or more file names or folders that you want to scan and click the right mouse button. A Windows NT shortcut menu containing the **Command AntiVirus Scan** option appears. Select that option by using either a right or left mouse click. The scan will begin immediately.

Another way to scan files quickly is through the Command AntiVirus drag and drop feature. To use this feature, you must have the Command AntiVirus interface open on your desktop. From Explorer or from the desktop, click the object you want scanned. Then, while holding the mouse button down, drag the files or folders anywhere over the Command AntiVirus window and release the mouse button. When the button is released, the scan starts immediately. When the scan ends, the system displays a report window.

For more information on the shortcut menu and the drag and drop feature, refer to **Quick Scanning** located in the *Command AntiVirus for NT Workstation User's Guide.*

MANUAL SCANS

Command AntiVirus for NT Workstation safely removes viruses from documents, boot sectors and partition tables. After installation, you can start a manual scan by clicking the desired task name and then clicking the **Execute Task** button. This starts a scan that, by default, gives a report if a virus is found. Should a virus be detected, disinfection will not occur until the action to take is modified. This can be done by selecting a task name, clicking the **Properties** button, and then selecting the **Action to take** pull-down menu.

CUSTOM SCANS

Command AntiVirus for NT Workstation comes configured with standard scanning tasks. You can create your own custom scan quickly and easily by clicking the **New Task** button and naming the task. The system displays the **Properties** dialog box. From here, you can select the action to take, the drive/path to scan, and the files to scan. You can also set up a schedule.

DYNAMIC VIRUS PROTECTION

Dynamic Virus Protection (DVP) provides on-access protection against viruses by scanning the boot sector every time a diskette is read and scanning every program file prior to execution. From the **Preferences/Active Protection** menu, you can enable or disable DVP and select whether to scan diskette drives, local hard drives, or network drives. You can also select the action to take on infection.

DVP, the kernel-mode driver that provides the on-access protection, actually consists of three drivers:

1. CSS-REC.SYS takes care of file systems and media changes.
2. CSS-FLTR.SYS handles events such as opens, closes and renames.
3. CSS-DVP.SYS is the scan engine.

VIEWING SCAN RESULTS

SCAN RESULTS LOGGED IN EVENT VIEWER

If Command AntiVirus finds a virus during a scheduled scan or on-access (using DVP), it logs the occurrence to the Windows NT Event Viewer. Viruses found by DVP are logged to Event Viewer's System log and viruses found during scheduled scans are logged to the Application log.

DISPLAYING SCAN RESULTS IN REAL-TIME

If you are using Windows NT 4.0, the **Real-time and Scheduled Scan Statistics** dialog box lets you see the results and the number of files scanned during scheduled scans and real-time (DVP) scans.

If you would like to view scanning statistics, position your cursor over the F-Agent icon (the yellow **C**) in the Windows NT task tray. Using the right mouse button, right-click to select the icon. When the shortcut menu appears, select **Get Statistics**. The system displays the **Real-time and Scheduled Scan Statistics** dialog box.

VIEWING RESULTS OF MANUAL SCANS

Statistics for manual scans (scan tasks initiated directly from the Command AntiVirus window) appear in the **Scan Results** window that appears when the scan completes.

MESSAGING CAPABILITIES

Command AntiVirus provides enterprise-wide messaging capabilities, including electronic mail, that utilize MAPI (Messaging Application Programming Interfaces).

AUTOMATIC UPDATE

This option allows system administrators to automatically perform partial or full-product updates of Command AntiVirus on each workstation when the user starts the computer. **Automatic Update** also allows each user to manually update a workstation. For more information, refer to **Automatic Update** located in the ***Network Administration*** chapter.

REMOVING COMMAND ANTIVIRUS

If you want to remove Command AntiVirus for NT Workstation from Windows NT 4.0, follow these directions:

1. Double-click **My Computer**.
2. Double-click **Control Panel**.
3. Double-click **Add/Remove Programs**.
4. Click **Command AntiVirus for NT Workstation**.
5. Click **Remove**.
6. Follow the default suggestions on the screen.

To remove Command AntiVirus from Windows NT 3.51, you **must** use FPUNINST.EXE (installed in the F-PROTNT directory) from the DOS command prompt. The following example assumes that the software is installed to the default location, C:\Program Files\Command Software\F-PROTNT. From the DOS prompt go to the F-PROTNT directory and type:

```
FPUNIST PROGRA~1\COMMAN~1\F-PROTNT
```

CSAV FOR NT SERVER

SYSTEM REQUIREMENTS

To operate Command AntiVirus for NT Server, you must have Microsoft Windows NT® Server edition 3.51 or higher installed on an IBM-compatible 386/25 computer with at least 16MB of RAM and 4MB of available hard-disk space.

INSTALLATION

NOTE: We strongly recommend that you exit all Windows programs before running the setup program.

There are two sets of installation instructions: Standard Installation and Setup for Network Administrators. Choose the one that is best suited for your situation.

STANDARD INSTALLATION INSTRUCTIONS

To install Command AntiVirus, you must be logged on as a member of the local administrators group.

1. Insert the CD-ROM.
2. Click the **Start** button (NT 4.0) or pull down the **File** menu of Program Manager (NT 3.51).
3. Click **Run**.
4. Select **Browse** to search the CD for the **NTSERVER** directory.
5. Change to that directory.
6. Double-click **SETUP.EXE** and click **OK**.

7. Select either the **Default** or the **Custom** configuration. The **Default** installation allows users to set up Command AntiVirus for NT Server on their local computers. **Custom** lets you select the components that you want installed.
8. The next dialog box that appears is the **Service Account for Network Scans**. There is a check box at the bottom that says "I'd like to be able to schedule scans of network drives".

   By default, the box is selected. If you clear this check box, scanning of network drives will be limited to manual scans. If you clear the check box and click **Next**, the installation begins. If you do not clear the check box, a **Command Software AV Scheduling Service** dialog box opens.
9. In the **AV Scheduling Service** dialog box, the current user information is displayed by default. If you are using your current account, enter your current password. If you want to change the information, use an account that meets the following criteria:

   A. The Username must reflect an existing account.
   B. The account must have rights to access network drives.
   C. Scanning requires that the user has **Read** access. To disinfect, quarantine or delete, the user must have **Write** access.

NOTE: If possible, use a password that does not expire. If you change the password for this account, you must change it in Command AntiVirus (**Preferences|Advanced|Service Account**). If your password expires, scheduled scans will not function on network drives.

If you enter an account that does not exist or if you enter an invalid password, Command AntiVirus will not validate the service account. As a result, scans of network drives will not take place. Also, Windows NT's Event Viewer will log a message regarding the invalidated service account.

Manual scans of local and network drives are allowed and DVP is active by default.

10. You are asked if you want to make a rescue disk. If so, insert a **virus-free** diskette into the diskette drive. Command AntiVirus formats the diskette and adds the necessary files.

NOTE: Select **No** when asked to format another diskette.

11. When SETUP is complete, the system displays the **Setup Complete** dialog box. Select **Finish** and you are done!

NOTE: If you are using diskettes, insert Disk #1 into drive A. After you have completed Steps 2 and 3, type **A:\setup** and press **Enter**. To complete the installation, continue to Step 7.

During the installation, the system prompts you for the additional diskettes.

SETUP FOR NETWORK ADMINISTRATORS

The **NETADMIN** parameter can be added to the command line when installing Command AntiVirus for NT Server. Using this command sets up an area on the network for administrators to install from so that individual diskettes are not needed for other server installations. Plus, by using the **NETADMIN** command, the System Administrator can control some key functions of Command AntiVirus. Some of these functions include preventing the disabling of real-time protection, restricting manual scans of network drives, and disabling the disinfection of viruses.

To use this capability, follow these steps:

1. Insert the CD-ROM.
2. Click the **Start** button (NT 4.0) or pull down the **File** menu of the Program Manager (NT 3.51).
3. Click **Run**
4. Select **Browse** to search the CD for the **NTSERVER** directory.
5. Change to that directory.
6. Click **SETUP**. The Run dialog box appears with the word SETUP.
7. Add a space and type **NETADMIN**.
8. Press **Enter**.
9. The system displays the Welcome screen and then the **Network Setup Configuration** dialog box.

   Enter the location on the network where you want to store the shared components of Command AntiVirus. Use a Universal Naming Convention (UNC) path that does not include spaces. This is necessary because InstallShield's SETUP.EXE is a 16-bit application and spaces included in a path will cause an error. The following is an example of a valid UNC path:

   ```
   \\SERVER\SHARED\INSTALL\SHARE
   ```

These files include F-PROT.EXE, the .FPT files (Command AntiVirus Task), Help files, the readme file, and assorted .DLL's.

10. Enter the location for the SETUP components. This is the area on the network that users will access so that they can install Command AntiVirus. Use a UNC path that does not include spaces. This is necessary because InstallShield's SETUP.EXE is 16-bit application and spaces included in a path will cause an error. The following is an example of a valid UNC path:

    ```
    \\SERVER\SHARED\INSTALL\SETUP
    ```

11. There is a check box that controls whether you want users to be able to scan network drives. Decide which is best for you. If you clear the check box, go to Step 14.
12. Select **Next**.
13. The next screen lets you enter information about the account that users will use for scheduled scans of network drives. Use an account that meets the following criteria:

    A. The Username must reflect an existing account.
    B. The account must have rights to access network drives.
    C. Scanning requires that the user has **Read** access. To disinfect, quarantine or delete the user must have **Write** access.
    D. The account should be accessible for all users.

NOTE: If possible, use a password that does not expire. If you change the password for this account, you must also update it in Command AntiVirus (**Preferences|Advanced|Service Account**). If the password expires, scheduled scans will not function on network drives.

14. Select **Next**. Setup begins.
15. The **Command AntiVirus Config** dialog box opens. Fill in your name and company information.
16. Select **Options** to view or modify Command AntiVirus' capabilities. Select or clear the choices and then either click **OK** to save your settings or click **Cancel**.
17. Setup continues and a final dialog box opens to confirm that the installation was successful.

In the setup components location that you selected, there is a batch file called LSILENT.BAT that lets you install all components to another server.

By running LSILENT.BAT from the server, all the components necessary to run Command AntiVirus are automatically installed with **no** user intervention needed.

After installation, you can access Command AntiVirus by double-clicking the yellow **C** in the tray on the right side of the taskbar. Or, you can create a permanent shortcut as described next.

NOTE: If you are using diskettes, insert Disk #1 into drive A. After you have completed Steps 2 and 3, type **A:\SETUP NETADMIN**. To complete the installation, continue to Step 8.

During the installation, the system prompts you for the additional diskettes.

CREATING A SHORTCUT

If you are using Windows NT 4.0, you may want to create a shortcut for easy access to Command AntiVirus. There are many ways to create shortcuts. The following is one example:

1. Right click the **desktop**.
2. Click **New**.
3. Click **Shortcut**.
4. Select **Browse**.
5. Double-click **Program Files**.
6. Double-click **Command Software**.
7. Double-click **F-PROTNT**.
8. Select **F-PROT32.EXE** and then **Open**.
9. Select **Next** and then **Finish**.

In Windows NT 3.51, a program group containing the icons for Command AntiVirus will be created for your desktop.

CREATING A RESCUE DISK

If you did not create a Command AntiVirus rescue disk during installation, you can run the setup program again and one will be created automatically. You can also create one manually. Make sure that your system is **virus-free** before beginning this task.

If you prefer to make a Command AntiVirus rescue disk manually, refer to the **Installation** chapter in the *Command AntiVirus for NT Server Administrator's Guide*.

SCANNING FEATURES

Command AntiVirus for NT Server contains the following scanning features.

SCHEDULED SCANS

Command AntiVirus for NT Server includes a service (CSS AV Scheduler) that runs scheduled and inactivity scans in the background. With this feature, server operations are not interrupted while Command AntiVirus's protection operates invisibly behind the scenes. A scan may be scheduled for a specific day, week or month. You can specify the time you want the scan to occur, or you can schedule a scan to run after a specified time of inactivity.

To create a daily scheduled scan of your hard drive, select **Scan Hard Drives** and then click the **Properties** button. From the **Properties** screen, click the **Schedule** button and be sure the **Enable Scheduling** option has a check mark in it. Specify the time of day in 24-hour format with 00:00 indicating midnight. If the computer is **not** on during the specified time, scheduled scans will be skipped.

QUICK SCANS

Within Command AntiVirus for NT Server, you can activate a shortcut menu that allows you to perform fast and efficient virus scans of selected folders or files. The files or folder to be scanned can be located in Windows NT's Explorer, on the desktop, or within program groups.

To perform a scan from the shortcut menu, select one or more file names or folders that you want to scan and click the right mouse button. A Windows NT shortcut menu containing the **Command AntiVirus Scan** option appears. Select that option by using either a right or left mouse click. The scan will begin immediately.

Another way to scan files quickly is through the Command AntiVirus drag and drop feature. To use this feature, you must have the Command AntiVirus interface open on your desktop. From Explorer or from the desktop, click the object you want scanned. Then, while holding the mouse button down, drag the

files or folders anywhere over the Command AntiVirus window and release the mouse button. When the button is released, the scan starts immediately. When the scan ends, the system displays a report window.

For more information on the shortcut menu and the drag and drop feature, refer to **Quick Scanning** located in the *Command AntiVirus for NT Server Administrator's Guide.*

MANUAL SCANS

Command AntiVirus for NT Server safely removes viruses from documents, boot sectors and partition tables. After installation, you can start a manual scan by clicking the desired task name and then clicking the **Execute Task** button. This starts a scan that, by default, gives a report if a virus is found. Should a virus be detected, disinfection will not occur until the action to take is modified. This can be done by selecting a task name, clicking the **Properties** button, and then selecting the **Action to take** pull-down menu.

CUSTOM SCANS

Command AntiVirus for NT Server comes configured with standard scanning tasks. You can create your own custom scan quickly and easily by clicking the **New Task** button and naming the task. The system displays the **Properties** dialog box. From here, you can select the action to take, the drive/path to scan, and the files to scan. You can also set up a schedule.

DYNAMIC VIRUS PROTECTION

Dynamic Virus Protection (DVP) provides on-access against viruses by scanning the boot sector every time a diskette is read and scanning every program file prior to execution. From the **Preferences/Active Protection** menu, you can enable or disable DVP and select whether to scan diskette drives, local hard drives, or network drives. You can also select the action to take on infection.

DVP, the kernel-mode driver that provides the on-access protection, actually consists of three drivers:

1. CSS-REC.SYS takes care of file systems and media changes.
2. CSS-FLTR.SYS handles events such as opens, closes and renames.
3. CSS-DVP.SYS is the scan engine.

VIEWING SCAN RESULTS

SCAN RESULTS LOGGED IN EVENT VIEWER

If Command AntiVirus finds a virus during a scheduled scan or on-access (using DVP), it logs the occurrence to the Windows NT Event Viewer. Viruses found by DVP are logged to Event Viewer's System log and viruses found during scheduled scans are logged to the Application log.

DISPLAYING SCAN RESULTS IN REAL-TIME

If you are using Windows NT 4.0, the **Real-time and Scheduled Scan Statistics** dialog box lets you see the results and the number of files scanned during scheduled scans and real-time (DVP) scans.

If you would like to view scanning statistics, position your cursor over the F-Agent icon (the yellow **C**) in the Windows NT task tray. Using the right mouse button, right-click to select the icon. When the shortcut menu appears, select **Get Statistics**. The system displays the **Real-time and Scheduled Scan Statistics** dialog box.

VIEWING RESULTS OF MANUAL SCANS

Statistics for manual scans (scan tasks initiated directly from the Command AntiVirus window) appear in the **Scan Results** window that appears when the scan completes.

MESSAGING CAPABILITIES

Command AntiVirus provides enterprise-wide messaging capabilities, including electronic mail, that utilize MAPI (Messaging Application Programming Interfaces).

ACCOUNT MANAGER

Many administrators grant users only basic rights to the local machine or domain. Frequently, those rights do not include the ability to add services and/or device drivers to the system. However, administrators may want to grant some of their users, those who do not have administrative control on their

computers, the ability to install and update Command AntiVirus. This is accomplished by using a utility called CSS-AMGR.EXE.

CSS-AMGR, also known as **Command's Account Manager** modifies the rights of selected accounts so that they can install and/or update Command AntiVirus. CSS-AMGR then stores information about the modified account on the local computer. Command's Account Manager allows the updating and installation of only Command AntiVirus: it does **not** add any other rights to the user's account.

For more information, refer to **Using Command's Account Manager** in the *Command AntiVirus for NT Server Administrator's Guide*.

AUTOMATIC UPDATE

This option allows system administrators to automatically perform partial or full-product updates of Command AntiVirus on each workstation when the user starts the computer. **Automatic Update** also allows each user to manually update a workstation. For more information, refer to **Automatic Update** located in the ***Network Administration*** chapter.

CSS CENTRAL

CSS Central provides system administrators with an easy-to-use interface for distributing, updating and modifying Command AntiVirus from one location. From this central location, you can change your Preference settings as well as create and modify individual scanning tasks. Now it is easier than ever to install and update your Command AntiVirus software.

For more information, refer to the **CSS Central** chapter of this quick start guide.

REMOVING COMMAND ANTIVIRUS

If you want to remove Command AntiVirus for NT Server from Windows NT 4.0, follow these directions:

1. Double-click **My Computer**.
2. Double-click **Control Panel**.
3. Double-click **Add/Remove Programs**.
4. Click **Command AntiVirus for NT Server**.

5. Click **Remove**.
6. Follow the default suggestions on the screen.

To remove Command AntiVirus from Windows NT 3.51, you **must** use FPUNINST.EXE (installed in the F-PROTNT directory) from the DOS command prompt. The following example assumes that the software is installed to the default location, C:\Program Files\Command Software\F-PROTNT. From the DOS prompt go to the F-PROTNT directory and type:

```
FPUNIST PROGRA~1\COMMAN~1\F-PROTNT
```

CSAV FOR NETWARE

SYSTEM REQUIREMENTS

To operate Command AntiVirus for NetWare, you need an IBM-compatible server with a minimum of an 80386 processor and 16 MB of RAM.

Command AntiVirus for NetWare protects Novell® NetWare 3.1x, 4.1x and 5.00. Command AntiVirus for NetWare runs independently of both the bindery and NDS. The NLM requires approximately 400K of RAM plus 53K per buffer.

Command AntiVirus for NetWare Administration program is compatible with Windows® 3.1x, Windows® 95 and Windows NT®.

INSTALLATION

This section guides you through the installation of Command AntiVirus for NetWare onto your NetWare server. Installation can be accomplished either through Windows or at the file server console. Do not attempt simply to copy the files to the server.

WINDOWS

Running **Setup** from Windows at a workstation allows you to install the NLM's to the server and the Windows program, Command AntiVirus for NetWare Administration, to the server or workstation.

1. Insert the CD-ROM into the CD-ROM drive on a workstation.
2. From the workstation, log in to the server with an ID that has full rights to SYS:SYSTEM and to the directory where Command AntiVirus Administration is to be placed. This allows the installation routine to create subdirectories and copy files to the correct locations.

3. From within Windows 3.x, click **File** and then **Run**. Or, if you are using Windows 95, click the **Start** button and then **Run**.
4. Select Browse to search the CD for the **FPN** directory.
5. Change to that directory.
6. Double-click **SETUP.EXE** and click **OK**.
7. Setup displays the Welcome screen. Click **Next**.
8. Setup displays a list of components to install. All components are selected by default. If you do not want to install a particular component, you can clear the appropriate check box. Click **Next**.
9. Setup displays the default installation directory for the workstation components. You can change this directory by specifying a new path. Click **Next**.
10. Setup displays a list of program folders. You can specify a program group for the Command AntiVirus Administration icons. The default is "Command AntiVirus." Click **Next**.
11. After installing some files, Setup displays a list of NetWare servers. You can select one or more servers on which to install CSAV for NetWare and AlertTrack ™. When you select a server, setup creates a subdirectory called F-PROT under SYS:SYSTEM, and the Command AntiVirus files are copied to this new directory. F-PROT.NLM, TTCONFIG.NLM, F-DELAY.NLM, and ALERTTRK.NLM are placed in SYS:SYSTEM. Other AlertTrack server files are in SYS:ALERTTRK. Click **OK**.

NOTE: Setup will only be able to copy files onto a server on which you are or can be logged into.

12. After installing some files, Setup displays the first of a series of information dialog boxes. Read the information contained in the box and click **OK** to continue. After the Command AntiVirus files are installed, you will be prompted to choose between restarting now or restarting later.
13. If you are loading Command AntiVirus for NetWare for the **first** time, you must now go to the file server to load Command AntiVirus. Type:

```
LOAD F-PROT
```

NOTE: On NetWare 4.x servers, it is normal to see the following message:

"The F-PROT.NLM NLM has registered a file system hook (x)"

You can toggle to the Command AntiVirus screen from the server console using **Alt + Esc**. These screens can be used to monitor Command AntiVirus for NetWare's status.

NOTE: The first time you load F-PROT. NLM, the **Daily** scan is created and then begins. If you do not want to run this scan, type the following load option:

```
LOAD F-PROT -DailyScan
```

This load option will work only if there is no INI file. When the NLM is first loaded, the INI file does not exist. The -DailyScan load option may also be used if the INI file has been deleted or moved.

14. Type:

```
LOAD ALERTTRK
```

NOTE: AlertTrack™ Lite installs two components. One program is a Windows workstation Management Console Program; the other is the AlertTrack NLM. After you have installed the AlertTrack™ NLM, you will be able to set up the necessary device configurations and recipient list for notifications from the management console at the workstation.

NOTE: If you are using diskettes, insert Disk #1 into drive A. After you have completed Steps 2 and 3, type **A:\SETUP** and press **Enter**. To complete the installation, continue to Step 7.

During the installation, the system prompts you for the additional diskettes.

CONSOLE INSTALL

This procedure does not install the Windows program Command AntiVirus for NetWare Administration.

1. Insert the CD-ROM into the CD-ROM drive on the file server.
2. Search the CD for the **FPN** directory.
3. Change to that directory.
4. At the server console, type:

   ```
   LOAD X:SETUP [ENTER]
   ```

   The letter X represents the volume name of your CD-ROM drive.

NOTE: There are two parameters that you can add when using this procedure:

A. If you do not want the install program to modify the server's AUTOEXEC.NCF file, add a minus "A" at the end of the command. For example:

```
LOAD X:SETUP -A [ENTER]
```

The letter X represents the volume name of your CD-ROM drive.

B. By default, a daily scan will be created and run when you first install CSAV. If you do not want this scan to be created, enter the following:

```
LOAD X:SETUP -S [ENTER]
```

The letter X represents the volume name of your CD-ROM drive.

You can combine both the -A(utoexec) and the -S(can) when using the LOAD X:SETUP command. For example:

```
LOAD X:SETUP -S -A [ENTER]
```

The letter X represents the volume name of your CD-ROM drive.

When the installation is complete, you will see the following message:

```
"Command AntiVirus for NetWare has been installed!"
```

NOTE: On NetWare 4.x servers, it is normal to see the following message:

"`The F-PROT.NLM NLM has registered a file system hook` (x)"

You can toggle to the Command AntiVirus screen from the server console using **Alt + Esc**. These screens can be used to monitor Command AntiVirus for NetWare's status.

NOTE: If you are using diskettes, insert Disk #1 into drive A and continue to Steps 4. Remember to substitute drive letter A: for X:.

During the installation, the system prompts you for the additional diskettes.

SCANNING FEATURES

After installation, all scanning, reporting and notification methods are ready-to-go. It is not necessary to make changes to the existing configurations. If you leave the default settings, you will have a daily scan that occurs at midnight. You will also have real-time protection active so that the server cannot become infected between scans. If a virus is found, the infected file is renamed and the results of scans are recorded in the Command AntiVirus log file.

The following options are for specific needs. Check the **Help** files for details. We suggest that you explore and test the program before making changes.

LOAD-TIME OPTIONS

There are load-time options that can be used when loading CSAV. To view these options from a help screen, type **Load F-PROT help** at the system console prior to loading CSAV.

CONSOLE COMMANDS

CSAV can be controlled either at the file server by console commands or by using the Windows program, Command AntiVirus for NetWare Administration.

If you prefer to use console commands, a help screen that lists the commands is available at the server console. To view the help screen, type **F-PROT** and press **Enter**. You can also access it remotely using RCONSOLE as long as REMOTE.NLM and RSPX.NLM are loaded. However, you cannot create scheduled scans with the console commands.

WINDOWS

If you prefer to work in Windows, use the CSAV Administration program. Its main screen lets you access all of the menu selections and also provides a means to control the servers in your domain. Additionally, there are screens that provide instant information pertaining to real-time scans and valuable server information.

MENUS

Task Menu

The **Task** menu allows you to customize the ready-to-go real-time, manual and scheduled scans and also lets you create new scanning tasks.

Deploy Menu

The **Deploy** menu provides the ability to propagate your settings automatically to all servers in your domain. It can also deploy updates for the NLMs and macro definition files across an entire domain of NetWare servers. CSAV **must** be loaded and running on each target server.

View Menu

Each server running CSAV maintains a separate log file called the Command AntiVirus log. This file records viral attacks, the action taken, and summaries of scheduled and manual scans. There is a **View** menu in the CSAV Administration program that allows you to see the Command AntiVirus log.

Notification Menu

Notification, located in the **Setup** menu, provides multiple options for real-time alerting through access to AlertTrack Lite.

Advanced Menu

The **Advanced** menu lets you create scan tasks and reporting templates to change new and/or existing tasks globally. There are also menu selections for unloading CSAV and reinitializing it to its defaults.

USING THE DEPLOY FEATURE

The **Deploy** pull-down menu allows you to implement scan configuration changes and updates to multiple servers quickly and easily. For more information, refer to **Deploy** in the *Command AntiVirus for NetWare Administrator's Guide*.

REMOVING COMMAND ANTIVIRUS

You can remove Command AntiVirus for NetWare by using the **DEINSTALL** command. This may only be done at the file server console or by using RCONSOLE. A complete description follows.

When you use the **DEINSTALL** command, F-PROT.NLM is unloaded, and **all** files and directories are deleted from:

```
SYS:SYSTEM\F-PROT

THE CURRENT QUARANTINE DIRECTORY WHICH IS BY DEFAULT
SYS:SYSTEM\F-PROT\QUARANT.INE

FILES RELATED TO COMMAND ANTIVIRUS WILL ALSO BE DELETED
FROM SYS:SYSTEM.
```

As the deinstall will delete **all** files from the quarantine directory, move any infected files that you want to keep to a safe place.

You **must** reinstall to have Command AntiVirus for NetWare's protection.

To begin the **DEINSTALL** you **must** be at the file server console or have RCONSOLE loaded.

1. Type **F-PROT DEINSTALL**

   The system displays the following message at the bottom of the screen. (There will be other information above the message, depending on what was occurring when you began the deinstall.)

   ```
   DEINSTALLING COMMAND ANTIVIRUS WILL REMOVE ALL FILES
   AND DIRECTORIES ASSOCIATED WITH COMMAND ANTIVIRUS.
   THIS WILL TAKE SOME TIME AND THE SYSTEM CONSOLE WILL
   BE LOCKED WHILE DEINSTALLING.  PROCEED?  Y/N
   ```

2. Type **Y** to continue. If you press **N**, the system displays the following message:

   ```
   "COMMAND ANTIVIRUS FOR NETWARE HAS NOT BEEN DEINSTALLED."
   ```

3. You will be prompted to enter a password. This is the same password you selected in Command AntiVirus Administration. If you have not selected one, use the default password ("password").

4. The system displays the following prompt:

   ```
   ENTER 'Y' TO BEGIN THE DEINSTALL, THIS COULD TAKE A
   WHILE AND THE SERVER CONSOLE WILL BE LOCKED UNTIL
   COMPLETE. BEGIN? (Y/N):
   ```

If you select **Y**, the system begins deleting all Command AntiVirus and Quarantine directories and everything in them.

5. When the procedure is complete, the system displays the following message:

```
COMMAND ANTIVIRUS FOR NETWARE HAS BEEN DEINSTALLED,
THANK YOU FOR GIVING US A TRY.

F-PROT IS UNLOADED
```

The deinstall process removes the "Load F-PROT" line from the AUTOEXEC.NCF file. The original AUTOEXEC is saved in a file called AUTOEXEC.FPN. Review these changes to insure proper operation.

The deinstall process does not remove AlertTrack. If you want to remove a default installation of AlertTrack, perform the following steps manually:

1. At the server console, type:

```
LOAD ALERTTRK /CLEAN
```

   Or, if you are running with bindery emulation on a NetWare 4.x or 5.x server, type:

```
LOAD ALERTTRK /CLEAN /BINDERY
```

2. Delete all files from SYS:ALERTTRK and remove the directory.
3. Delete ALERTTRK.NLM from SYS:SYSTEM
4. Delete the following load command from AUTOEXEC.NCF.

```
LOAD ALERTTRK
```

5. At the workstation, delete all AlertTrack files and any icons on the desktop.

CSS CENTRAL

CSS Central provides system administrators with an easy-to-use interface for distributing, updating and modifying Command AntiVirus from one location. From this central location, you can change your Preferences settings as well as create and modify individual scanning tasks. Now it is easier than ever to install and update your Command AntiVirus software.

CSS Central can be used to administer the following:

- Command AntiVirus v4.5 and later for Windows 95
- Command AntiVirus v4.5 and later for Windows NT 3.51/4.00 Workstation
- Command AntiVirus v4.5 and later for Windows NT 3.51/4.00 Server

The CSS Central main window contains two panes. The left pane is a tree view that always contains a computer group called CSAV Neighborhood. This view displays all of the computers that are available. The right pane reflects the current selection in the tree view.

Administrators can create their own groups and add computers to the group by dragging and dropping in the tree view. A computer group can contain computers or even other computer groups. For simplicity of administration and implementation, an individual computer can reside in only one computer group.

Selecting a computer in the tree view changes the display in the right pane to reflect the details of that selection. This is helpful for making comparisons of the settings.

For more information on CSS Central refer to the *Command AntiVirus for Windows NT Server Administrator's Guide*. This information is also available in the Command AntiVirus for Windows NT Workstation and Command AntiVirus for Windows 95 manuals.

SYSTEM REQUIREMENTS

CSS Central can be run on Windows NT server and workstation version 4.0 and above and on Windows 95.

NOTE: You cannot install CSS Central on versions of Windows NT prior to 4.0. However, servers and workstations running NT 3.51 can be administered.

NT workstation has a limitation of 10 inbound connections that can occur simultaneously (for more details see Article ID:Q122920 in the Microsoft Knowledge Base). Since CSS Central operates primarily on outbound connections, this should not be an issue if run from a workstation.

We have chosen TCP/IP and IPX/SPX protocols. TCP/IP or IPX/SPX **must** be configured and running on the computer running CSS Central. Also, TCP/IP or IPX/SPX **must** be running on the computer to be administrated.

F-AGENT from version 4.5X of Command AntiVirus **must** be active on the workstation that you administer.

CSS Central supports a first-time installation.

INSTALLATION

The following instructions allow you to install CSS Central quickly and easily using the default options.

INSTALLING

NOTE: We strongly recommend that you exit all Windows programs before running the setup program.

1. Insert the CD-ROM.
2. Click the **Start** button.
3. Click **Run**.
4. Select **Browse** to search the CD for the **CCENTRAL** directory.
5. Change to that directory.
6. Double-click **SETUP.EXE** and click **OK**.
7. After startup, the system displays the Welcome screen. Click **Next**.
8. Click **Next**.

9. Select **Default** from the **Setup configuration** screen. CSS Central begins the installation process.
10. Follow the instructions on the screen.

NOTE: If you are using diskettes, Insert Disk #1 into drive A. After you have completed Steps 2 and 3, type **A:\setup** and press **Enter**. To complete the installation, continue to Step 7.

During the installation, the system will prompt you for the additional diskettes.

OPERATING FEATURES

When you open a product configuration database, the CSS Central window contains the following operating features.

LEFT PANE

The left pane displays a tree view. There is always one computer group called **CSAV Neighborhood** that shows in the tree view. This group contains all other computers and computer groups.

Both computers and computer groups have a product configuration associated with them. This configuration consists of system-wide settings called **Preferences** and system tasks that are named for the task they represent.

Preferences

You can have zero or **one** Preferences item per computer or computer group. This item displays with the preference icon and the label **Preferences**.

CSS Central comes with a default configuration for Preferences which is applied to all computers. You can change this configuration for a specific computer or group of computers through the inherited configuration mechanism. For more information, refer to the Help files.

Task

You can have zero or more task items per computer or computer group. This item displays with a task icon and a label that is the name of the task.

When you add a task item, the item becomes a part of the configuration for all other computers. You can change this configuration for a specific computer or group of computers through the inherited configuration mechanism. For more information, refer to the Help files.

Computer Group

You can have zero or more computer group items per computer group. This item displays with a computer group icon and a user-defined label. If this group was created by adding a domain, the group will initially have that domain's name.

Computer

You can have zero or more computer items per computer group. This item displays with an icon that includes the operating system platform and version that the computer is running. For computers of unknown type, there is a computer icon with a question mark that identifies the computer type as unknown. The label is the computer name.

RIGHT PANE

The right pane reflects the current selection in the tree view and is read-only.

SINGLE CLICK

Selecting an item in the tree view affects the appearance of the list view displayed in the right pane.

DOUBLE-CLICK

When you double-click a group or computer icon in the tree view, a new window opens with a list view similar to the one in the right pane. All settings are read-only. The purpose of the new window is to make comparisons of existing settings.

If you double-click a task, a read-only window opens with a list of setting descriptions and values.

NOTE: If you use Windows NT, you can modify system tasks but not user tasks.

Under Windows 95, you can modify tasks created by CSS Central.

RIGHT MOUSE CLICK

When you click the right mouse button after selecting any of the items in the tree view, a menu is displayed. Different menu items are available depending on which item you select. If the option is not available for the selection, the text appears dimmed.

To view a dialog box that is identical to the task properties in the Command AntiVirus program, click the right mouse button on a task item and then select **Task Properties**. CSS Central creates and modifies system tasks.

DRAG AND DROP

An item can be moved in the tree view by dragging. To move settings, tasks, computers and computer groups, select the item you want to move, press and hold down the left mouse button and drag the item.

To copy settings and tasks, select the item, press and hold down the **CTRL** key, and then press and hold down the left mouse button and drag the item. Computers and computer groups cannot be copied.

MENUS

There are two views that can be displayed. One view displays when there is no product database open. The other displays when a product database is open.

When a product database is **not** open, the available options are:

File Menu

This **File** menu allows you to create, open or reopen a product configuration database.

View Menu

This **View** menu allows you to turn the status bar on or off.

Help Menu

The **Help** menu allows you to display help topics or information about CSS Central.

When a product database **is** open, the available options are:

File Menu

In addition to allowing you to create, open and reopen a product configuration database, this **File** menu allows you to close and save the current database. You can also update remote configurations.

Edit Menu

The **Edit** menu allows you to add, delete, rename, and find a computer or workgroup in the tree view. You can also purge or add a Preferences node, create a task configuration item, create a computer group, and lock or unlock a computer.

View Menu

In addition to allowing you to turn the toolbar and/or the status bar on or off, this **View** menu allows you to create new Item List, Settings, and Task Settings views. You can also display tab-controlled dialog boxes containing Network, Reporting, Active Protection, and Files to Include/Exclude settings dialogs.

Update Menu

The **Update** menu allows you to configure the FTP sites and platforms, download the latest version of Command AntiVirus, and automatically distribute the updates.

Remote Installation

The **Remote Installation** menu allows you to install or update files through an e-mail sent to an end user. The e-mail note contains an executable file called LOADER.EXE. When the recipient executes this program, it will determine the host operating system and launch the appropriate installation for CSAV.

Window Menu

The **Window** menu allows you to organize the windows on your desktop.

Help Menu

The **Help** menu allows you to display help topics or information about CSS Central.

REMOVING CSS CENTRAL

If you want to remove CSS Central, follow these directions:

1. Double-click **My Computer**.
2. Double-click **Control Panel**.
3. Double-click **Add/Remove Programs**.
4. Click **CSS Central**.
5. Click **Remove**.
6. Follow the default suggestions on the screen.

NETWORK ADMINISTRATION

This chapter covers network administration techniques for installing, upgrading, and operating Command AntiVirus. These techniques can be combined to support local workstations and off-site users.

For example, you can place Command AntiVirus on the server and then users can install the program to their local hard drives. For more information about this interactive installation, refer to **Installing from the Server**.

You can also update Command AntiVirus automatically, with no user interaction, to numerous workstations from a server. This process is completed through our Automatic Update feature. For more information about Automatic Update, refer to **Automatic Update**.

Scanning can also be automated. For example, you can install Command AntiVirus on a server and run a local DOS virus scan when the user logs in. This technique is helpful when workstation drive space is limited or when configuring each workstation separately is inconvenient. To learn more about this scanning technique, refer to **Running A DOS Scan At Login**.

To provide system protection against new viruses, we update Command AntiVirus frequently. You can download interim releases from our web, FTP and BBS sites.

To protect your systems, be sure to keep your copy of Command AntiVirus updated. For more information about installing the program from a downloaded version, refer to **Installing Command AntiVirus From the Server**.

In addition to providing instructions in how to set up Command AntiVirus for network administration, this chapter also covers some of the additional tools and techniques available to administrators. Some of these tools include:

- Restricting users from disinfecting their workstations.
- Preventing workstations from scanning network drives.
- Using the administrative utility programs and special batch files that come with Command AntiVirus.
- Broadcasting and controlling virus alert broadcast messages.

INSTALLING COMMAND ANTIVIRUS FROM THE SERVER

This method allows each workstation to install Command AntiVirus manually from the server without using any installation diskettes.

USER-INITIATED INSTALLATIONS

There are two special batch files that you can use to simplify the server-based distribution process, NETDISK.BAT and ONEDISK.BAT. After you have set up a shared directory on a network of your choice, both batch files copy the installation files to that directory. Once the files are in place, users can go to this installation directory and run either SETUP or INSTALL to have Command AntiVirus install to their local workstations.

Choose NETDISK.BAT if you are working from the installation diskettes you have received from Command Software. Choose ONEDISK.BAT if you have downloaded a version from our BBS or FTP site.

Using NETDISK.BAT

NETDISK.BAT is on the installation diskettes that you have received from Command Software.

NOTE: You must run NETDISK.BAT from the server. By doing so, the files needed for server-to-workstation installation can be copied to a shared directory.

To use NETDISK, follow these steps:

1. Create a shared F-PROT directory on the server and then change to that directory.

2. Insert the Command AntiVirus Installation Disk #1 into drive A of your workstation or server.
3. Copy NETDISK.BAT from the drive A to the shared directory that you created in Step 1.
4. From within the shared directory, type the following command:
   ```
   NETDISK A:
   ```
5. Press **Enter**. The system displays a brief instructional screen.
6. When you have finished reading the instructions, press **Enter** to continue.
7. Insert Command AntiVirus Installation Disk #1 into drive A.
8. Follow the screen instructions. When the copying is complete, any user with access to the shared directory created in Step 1 can run INSTALL from DOS or SETUP from Windows to perform a standard installation of Command AntiVirus from the server to the user's local hard drive.

Using ONEDISK.BAT

Although ONEDISK.BAT is similar to NETDISK.BAT, you use ONEDISK.BAT with downloaded versions of Command AntiVirus, not with installation CD-ROM or diskettes.

If you download Command AntiVirus, you will receive a large executable file.

To use this file, you need to place it in a separate, temporary directory and run it. When you run the downloaded file, it produces several other files, one of which is ONEDISK.BAT.

The following instructions will help you use ONEDISK.BAT.

You can also find instructions for using ONEDISK.BAT in INSTALL.DOC, which is contained in the downloaded file.

1. Create a shared directory on the server for Command AntiVirus installation files.
2. Change to the temporary directory that contains the downloaded files. For example, at the command line type:
   ```
   CD C:\DOWNLOAD
   ```
3. Press **Enter**.

4. Type ONEDISK followed by the drive and path of the shared directory that you created in Step 1. For example, if you created the directory, F-PROT, in the PUBLIC directory on drive F, at the command line type:

   ```
   ONEDISK F:\PUBLIC\F-PROT
   ```

5. Press **Enter**. When the copying is complete, any user with access to the shared directory that you created in Step 1 can run INSTALL from DOS or SETUP from Windows to perform a standard installation of Command AntiVirus to their local hard drive.

AUTOMATIC UPDATE

If you have several workstations, each with a different operating system, you can perform a partial or full-product update of Command AntiVirus on each station directly from a server by using our Automatic Update feature. This feature provides system administrators with the ability to distribute and update the program quickly on multiple workstations in a multi-platform environment with no user interaction.

Automatic Update operates by placing Command AntiVirus files in a unique parent directory in a shared location on the network. When the user starts the computer, the Automatic Updates process compares the dates of the files on the workstation with those on the server. If the server dates are newer, the server responds by automatically updating the workstations with the newer program files.

For example, if only the definition (*.def) files have changed since the last update, then only those files will be updated. If a new version is available, then the program begins a complete SETUP.

Component updates are not visible to the user. At most, the user may notice that the system is a bit slower. With full-product updates, the system displays the SETUP screens, but no action is required.

NOTE: To use the Automatic Update feature, Command AntiVirus must be installed on each workstation. For new installations, you must run SETUP manually from the workstation, or use CSS Central to deploy new product.

The following instructions will help you use the Automatic Update feature:

1. In a shared location on the network, create a unique parent directory to store the update files. This directory is the **remote setup location**. For example:

   ```
   S:\NEWFPROT
   ```

2. Download and extract the latest definition files and copy them to the **remote setup location**.

3. Create a subdirectory for each platform to be updated. For example:
   ```
   S:\NEWFPROT\CSAV95
   ```

4. Copy **all** of the product files into their respective subdirectory. Although it is not necessary, it is helpful to create subdirectories under each platform directory to contain full product, component updates, and signature files. For example, you may want to create the following directory structure:

   ```
   S:\NewFPROT
   S:\NewFPROT\CSAV95
   S:\NewFPROT\CSAV95\FULL
   S:\NewFPROT\CSAV95\COMP
   S:\NewFPROT\CSAV95\PROD
   ```

5. Using Notepad or any text editor, create a file named CSSFILES.INI. For each platform specified in the automatic update directory structure, create a section in this .ini file. An example CSSFILES.INI file follows:

   ```
   [Win95-ANTIVIR]
   BaseDir=S:\NewFPROT\CSAV95
   FULLPROD=full\
   COMPONT=comp\
   DEFFILES=sign\

   [NT40_S-ANTIVIR]
   BaseDir=S:\NewFPROT\CSAVNTS
   FULLPROD=full\
   COMPONT=comp\
   DEFFILES=sign
   ```

NOTE: Universal Naming Convention (UNC) paths can be substituted for mapped drives. We recommend using UNC paths.

6. If you have not yet installed CSAV throughout the enterprise, follow Steps 7 through 10; otherwise, skip to Step 10.

7. Locate the SETUP.INI file and search for: AutoUpdateDir=
   In CSAV for Windows search for: RemoteUpdatePath=

8. Type **remote setup location** after the equal sign. For example:
   ```
   AUTOUPDATEDIR=S:\NEWFPROT
   ```

9. Save the changes.

10. CSAV is now ready to be installed throughout the enterprise. With the modifications just made, CSAV will be configured to check the NewFPROT directory at each login to search for new files to update. If CSAV is already installed and you want to modify workstations manually, follow Steps 11 through 15.
11. Open Command AntiVirus.
12. Click **Preferences**.
13. Click **Advances**. Click the **Automatic Update** dialog tab.
14. Click **Browse**. The system displays the **Browse Open** dialog box.
15. Select the drive\path of the **remote setup location**. For example:

    ```
    S:\NEWFPROT
    ```

    The directory path **must** point to the **remote setup location** which contains the CSSFILES.INI regardless of whether you are performing partial or full-product updates.

NOTE: When the drive\path selected is a network drive, the selection is converted to a Universal Naming Convention (UNC) path.

16. Click **OK**. The **Browse Open** dialog box closes.
17. Click **OK**. The update occurs automatically when the user restarts the computer or if the user leaves the computer on, between 4 a.m. and 5 a.m.

NOTE: Once you complete this process, workstations are updated automatically each time you place **updated** files in the **remote setup location** and **setup** subdirectory.

Component updates are not visible. At most, the user may notice that the system is a bit slower. With full-product updates, the system displays the SETUP screens, but the user does not need to take any action.

NOTE: If the updated files require that you restart your system for the changes to take effect, the system displays the following message:

```
"We have updated some files in this release. These
files and some settings will not take effect until
a reboot is performed.  In the interim your system
remains fully protected."
```

As soon as an update takes place, the program does not automatically update again for at least 24 hours. The **Update Now** button allows the user to update the individual workstation immediately.

There are no restrictions to prevent the user from changing the path of the **remote setup location**. If the user changes the path, the updates will be made from the path specified.

NOTE: To turn off the Automatic Update feature, leave the **remote setup location** blank. For more information about **Automatic Update** and **Update Now**, see **Automatic Update** in your Command AntiVirus manual.

RUNNING A DOS SCAN AT LOGIN

If you want to run a DOS scan on your workstations at login without actually having the program on the workstations, use the following instructions:

1. Install Command AntiVirus on a workstation hard drive. By default, the program files are installed to C:\F-PROT. This process allows you to copy the program files to a shared directory on the server.
2. Create a shared F-PROT directory on a server. For example, create an F-PROT directory in the PUBLIC directory on drive F. All users need **Read** and **File Scan** rights to this directory.
3. Copy all of the program files in the local directory, C:\F-PROT, to the shared directory, F:\PUBLIC\F-PROT, on the server.
4. For NetWare 3.1x, modify the LOGIN script with the following lines. For NetWare 4.x, you must use bindery emulation.

```
DOS SET FP-DATA="C:\F-PROT.DAT"
\PUBLIC\F-PROT\F-PROT /HARD /TODAY
```

The FP-DATA line is necessary because the daily scan option writes a very small data file that must remain on the local drive (or any drive to which the user has "write" access).

RESTRICTING NETWORK USERS

Many administrators want to restrict users from increasing the network load with repetitive or unnecessary scans. If a virus is found locally, an administrator may want to be notified in order to personally disinfect that workstation.

To help administrators in their efforts to restrict user intervention, Command AntiVirus includes the following specialized utility.

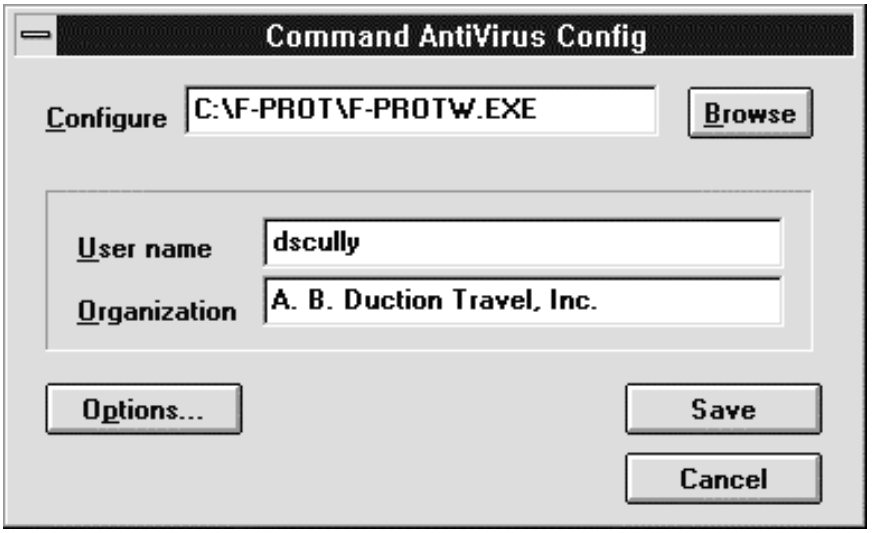
FPWCFG.EXE: CONFIGURING F-PROTW.EXE

You can use FPWCFG.EXE to modify Command AntiVirus for Windows executable file, F-PROTW.EXE. Modifying F-PROTW.EXE allows administrators to restrict the user's ability to scan network drives, to disinfect viruses, and to disable Dynamic Virus Protection (DVP).

To maintain administrator control over these actions, do **not** make FPWCFG.EXE available to your users.

After installing Command AntiVirus on the administrator's workstation, use the following instructions to modify FPROTW.EXE:

1. Run FPWCFG.EXE (you will find it on the installation diskettes) from within Windows. The system displays the following dialog box appears:



Command AntiVirus Config Dialog Box

2. Click on **Browse** and locate F-PROTW.EXE in the F-PROT directory.
3. Click on **Options**.
4. Select the Scan Network check box.
5. Clear the Allow Disinfection check box.
6. Click on **Save**. The system saves the changes that you made in the Command AntiVirus Config dialog box to the F-PROTW.EXE file.

You can now use the modified F-PROTW.EXE as part of the installation process. If users are installing from the server or if you want to change your diskettes, first use PKZIP to include the modified F-PROTW.EXE in the existing file, SE_FPRTW.EXE. (SE_FPRTW.EXE is an installation file). For example:

```
PKZIP SE_FPRTW.EXE F-PROTW.EXE
```

Command AntiVirus does not include PKZIP. PKZIP is available in many of the major shareware sites on the Internet.

After you have zipped F-PROTW.EXE into SE_FPRTW.EXE, copy the new SE_FPRTW.EXE either to the server's installation directory or to the diskette that will be used for installation. Any future installations that use the modified SE_FRPTW.EXE will contain the restrictions that you added to F-PROTW.EXE.

BATCH FILES

The following batch files provide options that will simplify the administrator's distribution tasks.

XDISK.BAT: CREATING INSTALLATION DISKETTES

After downloading the Command AntiVirus update file, you can use the XDISK.BAT file to create a set of high-density (1.44Mb) install diskettes. The letter **X** represents the number of diskettes; this is different for each platform.

Use the following instructions to create the diskettes:

1. Format the appropriate number of 3.5 inch, high-density diskettes and label them **Installation Disk #1**, **#2**, **#3**, etc.
2. Run XDISK.BAT with the destination drive as its only parameter.
3. In a DOS window, change to the folder that contains the installation files (make sure XDISK.BAT is there) and at the command line type:

   XDISK A:

   Or from the Start menu, use the Run dialog box and specify a path.
4. Press **Enter**. The system prompts you to insert a blank 3.5 inch diskette.
5. Insert **Installation Disk #1** and follow the on-screen instructions. The system prompts you for the remaining diskettes.
6. After copying the installation files, write-protect the diskettes.

You can use these diskettes to install Command AntiVirus as follows:

1. Insert **Installation Disk #1** into Drive A.
2. From the **Start** menu choose **Run** and type: **A:\SETUP**
3. Press **Enter**.
4. Follow the screen instructions to complete the installation of the program.

SCAN.BAT: LOGGING SCAN RESULTS LOCALLY

You can find SCAN.BAT in the self-extracting file, SE_SCAN.EXE, which is on Command AntiVirus installation diskettes. SCAN.BAT performs a DOS-based scan that allows you to send the scan or program-related information to a log file. The log file is located on the local drive. When you run SCAN.BAT, it calls on two files, FPROT.BAT and ERR-CHK.BAT.

Before running SCAN.BAT, you must create or modify the LOGIN script environment variables shown below, using the appropriate values:

```
[sample LOGIN script]
dos set NETNAME="FULL_NAME"   name assigned by SYSCON
dos set STATION="STATION"     connection number at file server
dos set NODE="P_STATION"      node address
```

FPROT.BAT copies these values into the file, LOGG, which is located on the local hard drive. You will need to modify the path in FPROT.BAT to reflect where the report will be saved on the server. LOGG is later appended to the network report generated by F-PROT.EXE.

To use SCAN.BAT, change to the directory containing this batch file and run the following command:

```
SCAN
```

AUTOMATED SCANNING

There are several programs on the Command Software Systems BBS and FTP site that you can use with batch files to create automated scans. The file TIME_COM.ZIP contains files that allow you to check for seconds, minutes, hours, days, a specific day of the week, month, and year. For example, one of these files, DOW.COM (Day Of the Week), was used to create the ONEWEEK.BAT file shown below, which scans once a week.

ONEWEEK.BAT

```
@ECHO OFF
REM ONEWEEK.BAT - WRITTEN BY CSS SPBPJN 9-27-94
REM TECHNICAL SUPPORT DEPARTMENT
REM This file is designed to only execute a series
REM of commands when a particular day is reached.
REM Only one day is used, therefore, only one day
REM out of the week can be specified.
REM NEEDED FILE:DOW.COM > RETURNS ERRORLEVEL 0 TO 6
REM THE CORRESPONDING NUMBERS FOR THE DAYS OF THE
REM WEEK ARE: SUN = 0, MON = 1, TUES =2, WED =3,
REM THURS = 4, FRI = 5, SAT =6
REM PLACE THE NUMBER FOR THE DAY OF WEE* YOU WANT
REM F-PROT TO RUN ON AFTER "SET DAY_TEMP=" LINE
REM CURRENTLY,F-PROT IS SET TO EXECUTE ON MONDAY.
SET DAY_TEMP=1
:DAYWEEK
DOW.COM
FOR %%V IN ( 0 1 2 3 4 5 6 ) DO IF ERRORLEVEL %%V SET OW_TEMP=%%V
IF %OW_TEMP%==%DAY_TEMP% GOTO ACTION
GOTO END
:ACTION
REM THIS IS WHERE YOU WANT TO INSERT THE DESIRED
REM STATEMENTS THAT WILL RUN ON THE DAY SPECIFIED.
REM BELOW IS A SAMPLE LINE FOR THE F-PROT STATEMENT
REM TO BE INCLUDED WHICH YOU MAY WANT TO CHANGE. YOU
REM CAN ALSO ADD STATEMENTS BEFORE AND AFTER THE
REM F-PROT LINE FOR ITEMS THAT YOU WANT TO OCCUR
REM ON THE SAME DAY.
ECHO SCAN BEING PERFORMED
C:\F-PROT\F-PROT.EXE /HARD /DISINF
GOTO END
:END
REM CLEAR OUT VARIABLES
FOR %%V IN ( DAY_TEMP OW_TEMP ) DO SET %%V=
```

ON-ACCESS CONSIDERATIONS

On-access programs provide an important level of protection. If limited memory is a factor, you may need to configure your system(s) differently than the default settings. For more information, see the Command AntiVirus manual.