Multi-Platform Quick Start Guide

Command AntiVirusTM

For Windows® 3x, DOS, Microsoft® Exchange, and NetWare®

NOTICE

Command Software Systems, Inc. (CSSI) reserves the right to improve the product described in the companion 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

The Software is protected by United States copyright laws, international copyright treaties as well as other intellectual property laws and international treaties.

License Grants. Licensor (CSSI) hereby grants Licensee the non-transferable right to use, as set forth below, the number of copies of each version number and language of Software set forth on Licensee's valid proof of purchase.

For each License acquired, Licensee may use one copy of the Software on a "one user per license" basis, 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. A server License requires user access licenses on a "one user per access license" basis, or as defined with each server product.

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 or by executing same or similar electronically as part of the installation process, 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 media and the physical documentation to be free of defects with respect to materials and workmanship for a period of thirty (30) days from the date of purchase. During the warranty period, CSSI will replace the defective media or documentation. This warranty is limited to replacement and does not encompass any other damages. CSSI MAKES NO OTHER EXPRESS OR IMPLIED WARRANTIES INCLUDING THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE AND THE WARRANTY OF MERCHANTABILITY.

Published in the U.S.A. by Command Software Systems, Inc. All rights reserved.
Document No. MQS-480-0403

Part No. 07-9001-00

TABLE OF CONTENTS

INTRODUCTION

The Multi-Platform Quick Start Guide contains system requirements, installation instructions, and an overview of the following Command AntiVirus products:

- Command AntiVirus for Windows 3x
- Command AntiVirus for DOS
- Command AntiVirus for Microsoft® Exchange
- Command AntiVirus for NetWare®

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.commandsoftware.com.

This chapter includes a list of product features and conventions used throughout this quick start guide. It also contains details on accessing additional product-related information from the Command Software Systems web site.

MAIN FEATURES

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

- State-of-the-art technology to scan for tens of thousands of known viruses and their variants.
- Continuous on-access scanning (Dynamic Virus Protection) in Windows® and NetWare®.
- Scanning of compressed files and compressed executables.
- Save removal of viruses from files, boot sectors, and partition tables.
- Fully configurable inclusion/exclusion of files from the scan list.
- Enterprise-wide messaging capabilities including electronic mail.
- Companion product notification (Command AntiVirus for NetWare).
- ICSA certification for effective virus protection.

CONVENTIONS USED

⚠ Indicates an area that requires special attention.

✓ Indicates a helpful tip.

`COURIER` Examples and messages appear in `COURIER`. For example:

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

CSAV The acronym used for Command AntiVirus.

Italics A reference to the manual is in italics.

Italics A reference to another chapter in the manual is in bold and italics.

Bold A reference to a section within the chapter is in bold.

TESTING COMMAND ANTIVIRUS

For testing purposes, there is a self-extracting file called **SE_EICAR.EXE**. You can download **SE_EICAR.EXE** from our web site at **http://www.commandsoftware.com**.

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 antivirus protection properly and that Dynamic Virus Protection (DVP) (on-access) protection is working. **EICAR.COM** lets you create and safely test customized virus warning messages. It also provides a way to demonstrate how Command AntiVirus responds when it finds a virus.

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 95/98/Me, Windows NT, Windows 2000, and Windows XP 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 **Command AntiVirus for Windows – Dynamic Virus Protection Report** log. This log provides the details for **all** virus infections found.

NOTE: In Windows 3.1x, 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:

- Command Software U.S. – **http://www.commandsoftware.com**
- Command Software UK – **http://www.command.co.uk**
- Command Software Australia **– http://www.commandcom.com.au**

HELP

You can obtain help by selecting **Help** from the **Help** menu in the Command AntiVirus graphical user interface (GUI).

The Help menu item brings you to the Documentation download page of the Command AntiVirus web site. From there, you can view the documentation to find information about a specific topic, or you can download the documentation file.

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, fixes and special instructions is in the README.TXT file. You can review this file at the beginning of the installation, from the **Help** menu in the Command AntiVirus GUI, or on the Command Software Systems web site.

CSAV FOR WINDOWS 3X

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 80386 computer with at least 4 MB of RAM and 6 MB 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

The following instructions will help you to install Command AntiVirus for Windows quickly and easily using the default options. The **Typical** installation installs all of the components required for complete antivirus protection. The components are:

- **Command AntiVirus for DOS** – the DOS-based version of Command AntiVirus.
- **Command AntiVirus for Windows** – the Windows 3x version of Command AntiVirus.
- **Dynamic Virus Protection (DVP)** – on-access virus protection for Windows.
- **F-NET Components** – allows your computer to communicate with a server that is running Command AntiVirus for NetWare.
- **Command AntiVirus Quick Start Guide** – provides a brief overview of our products and basic start-up instructions. The guide is located in the file called MQCKST.PDF and can be viewed with Adobe® Acrobat® Reader.

A **Custom** installation allows you to select the components that you want to install. For more information, refer to the ***Installation*** chapter of the *Command AntiVirus for Windows User's Guide.*

TYPICAL INSTALLATION

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. Click **Browse** to search the CD for the **WIN3x** directory.
4. Change to that directory.
5. Double-click **SETUP.EXE** and click **OK**. After startup, the system displays the **Welcome** screen.

NOTE: Command AntiVirus requires the use of Win32s components. If these components are not installed on your system, Command AntiVirus prompts you to install them.

6. Click **Next**. The system displays the **Software License Agreement**.
7. Click **Yes**. The system displays the **Select components** dialog box.
8. Select **Typical**.
9. Click **Next**. The system displays the **Choose Destination Location** dialog box.
10. The default location is C:\F-PROT. Click **Next**.
11. The setup program begins copying the Command AntiVirus files to your system. When the copying is complete, the system displays the **Setup Complete** dialog box.

12. The default selection restarts Windows to activate your on-access protection. Click **Finish**.

After installing Command AntiVirus, we recommend that you perform a manual scan of your local drives to ensure that your system is **virus-free**.

CREATING A RESCUE DISK SET

NOTE: To create a rescue disk set, you **must** have the Command AntiVirus (CSAV) for DOS component installed on your system. CSAV for Windows installs this component by default.

The following instructions will help you create a rescue disk set. A rescue disk set allows you to run Command AntiVirus.

Make sure that you have **three** blank 3.5 high-density diskettes labeled **CSAV Rescue Disk 1 for (User's Computer ID)**, **CSAV Rescue Disk 2 for (User's Computer ID)**, and **CSAV Rescue Disk 3 for (User's Computer ID)**. Also, make sure that the diskettes and your system are **virus-free**.

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

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

2. Press **Enter**.
3. Insert **Rescue Disk 1** 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. As you already have a diskette in drive A, proceed to **Step 6**.
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 **Rescue Disk 1**, and insert **Rescue Disk 2** into drive A.
10. Press **Enter**. The system displays a warning that the diskette will be formatted.
11. Press **Enter**. The system prompts you to insert a diskette. As you already have a diskette in drive A, proceed to **Step 12**.
12. Press **Enter**. The system formats the diskette. When the formatting is complete, the system asks if you would like to format another diskette.
13. Type **N**.
14. Press **Enter**. The system begins copying the files.
15. When the system has finished copying the files, remove **Rescue Disk 2**, and insert **Rescue Disk 3** into drive A.
16. Press **Enter**. The system displays a warning that the diskette will be formatted.
17. Press **Enter**. The system prompts you to insert a diskette. As you already have a diskette in drive A, proceed to **Step 18**.
18. Press **Enter**. The system formats the diskette. When the formatting is complete, the system asks if you would like to format another diskette.
19. Type **N**.
20. Press **Enter**. The system begins copying the files.
21. **When the system has finished copying the files, remove** Rescue Disk 3 from drive A.
22. Set the write-protect tab on each diskette to prevent any modifications.

If necessary, you can run a Command AntiVirus scan from the rescue disk set.

Rescue Disk 1 contains the **FIXDISK** utility and the **RESCUE.DAT** file that contains a copy of the master boot record and boot sector.

As the rescue file on **Rescue Disk 1** is machine-specific, this diskette is for use only on the computer that was used to create the file.

You have just created a CSAV Rescue Disk set. Put the rescue disk set in a safe place. Be sure to update the set when you get your next Command AntiVirus update.

USING THE RESCUE DISK SET

Some viruses may prevent you from starting up your system or accessing your Command AntiVirus program. For example, you may need to repair damage or infected boot sector information.The **Rescue Disk** set helps you to detect and remove these viruses.

If you need to use the Rescue Disk set, follow these steps:

1. Turn off your computer.
2. Place a virus-free, write-protected bootable diskette into drive A.
3. Turn on your computer.
4. If you are prompted to enter a new date and a new time, press **Enter** for each.
5. Remove the bootable diskette and insert **Rescue Disk 1** into drive A.
6. At the A prompt, type the following:

```
F-PROT /HARD /DISINF /LOADDEF /ALL
```

7. Press **Enter**. The system prompts you to insert a diskette with **SIGN.DEF**.
8. Insert **Rescue Disk 2** into drive A and press **Enter**. The system prompts you to insert a diskette with **SIGN2.DEF**.
9. Insert **Rescue Disk 3** into drive A and press **Enter**. A scan of your hard drive begins immediately. If any viruses are detected, allow CSAV to disinfect them.
10. When the scan is complete, remove **Rescue Disk 3** from drive A.

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 *Command 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 displays.

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 so that the program runs 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 *Command 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.

Files to Include/Exclude

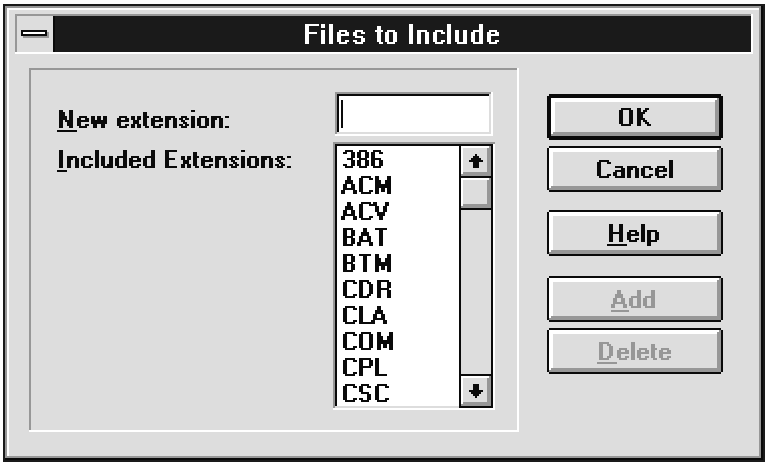
Through the **Options** menu in Windows, you can specify additional file types to **Include** in and what files to **Exclude** from all Windows-based scans.

NOTE: For the changes that you make to take effect immediately, you **must** exit Windows to DOS and then restart Windows.

NOTE: The **Files to Exclude** option cancels the **Include** option. For example, if the .DOC extension is listed in the **Included Extensions** list of the **Files to Include** dialog box and the **Filenames** list of the **Files to Exclude** dialog box contains an *.DOC all files with an extension of *.DOC are **not** scanned.

To access the **Files to Include/Exclude** dialog boxes, follow these steps:

1. On the menu bar, click **Options**. The system displays the drop-down menu.
2. Click **Files to Include/Exclude**. The system displays a submenu.
3. Click **Files to Include** or **Files to Exclude**. The system displays the appropriate dialog box:



Files to Include

Files to Include

Command AntiVirus contains hard-coded file types that are scanned by default. In Windows, these file types are displayed in the **Included Extensions** list of the **Files to Include** dialog box. They cannot be deleted.

To exclude a hard-coded file type from scans, add an asterisk and the file type’s extension to the **Filenames** list of the **Files to Exclude** dialog box. For example, to exclude all .DOC files from a scan, add *.DOC. Although the extension still appears in the **Included Extensions** list, files with that extension are **not** scanned.

This option also allows you to specify **20** user-defined file types for CSAV to scan. To add a file name extension to the list, type the extension in the **New Extension** text box and click **Add.** To remove an extension that you have added, select the extension and click **Delete**.

NOTE: In Windows, Command AntiVirus does **not** scan self-extracting files by default. Dynamic Virus Protection (DVP) scans the contents of the self-extracting file when the files are extracted. However, the .EXE portion of the self-extracting file is scanned by default.

To scan the contents of self-extracting files in zipped form, we recommend that you perform an on-demand scan of **Packed Files** during off-peak hours. To scan self-extracting and packed files, select the **Packed Files** check box in the **Targets to Scan** dialog box.

Files to Exclude

In Windows, this option allows you to specify which files CSAV does **not** scan. The files that are excluded from the scan are displayed in the **Filenames** list.

You can use wildcard characters to specify a file name. For example, to exclude all files with names starting with the letters abc, type:

```
ABC*
```

To add a file to the list, type the full file name and extension or wildcard combination in the **New Exclusion** text box and click **Add**. To remove a file, select the file from the list and click **Delete**.

NOTE: To exclude a hard-coded file type from scans, add an asterisk and the file type's extension to the **Filenames** list. For example, to exclude all .DOC files from a scan, add *.DOC. Although the extension still appears in the **Included Extensions** list of the **Files to Include** dialog box, files with that extension are **not** scanned.

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 CSAV for DOS **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 it does not scan files that are opened in DOS.

REMOVING COMMAND ANTIVIRUS

To remove Command AntiVirus for Windows, follow these steps:

1. In the Window’s Program Manager, double-click the **Command AntiVirus** program group.
2. Double-click the **Uninstall Command AntiVirus for Windows** icon. The system displays the **Confirm File Deletion** dialog box.
3. Click **Yes**. The system displays the **Remove Programs From Your Computer** dialog box.
4. When the system displays the “Uninstall successfully completed” message, click **OK**.

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 2 MB of RAM and 6 MB of available hard disk space.

You can use Command AntiVirus on a workstation connected to a Microsoft® 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, accept the default options.

INSTALLING

To perform a default installation, 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. Select **Install Command AntiVirus**.
6. Press **Enter**.
7. Follow the instructions 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, proceed to **Step 3**.

⚠ After installing Command AntiVirus, we recommend that you perform a manual scan of your local drives to ensure that your system is **virus-free**.

CREATING A RESCUE DISK SET

The following instructions will help you create a rescue disk set. A rescue disk set allows you to run Command AntiVirus.

Make sure that you have **three** blank 3.5 high-density diskettes labeled **CSAV Rescue Disk 1 for (User's Computer ID)**, **CSAV Rescue Disk 2 for (User's Computer ID**), and **CSAV Rescue Disk 3 for (User's Computer ID)**. Also, make sure that the diskettes 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 **Rescue Disk 1** 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. As you already have a diskette in drive A, proceed to **Step 6**.

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 **Rescue Disk 1** and insert **Rescue Disk 2** into drive A.
10. Press **Enter**. The system displays a warning that the diskette will be formatted.
11. Press **Enter**. The system prompts you to insert a diskette. As you already have a diskette in drive A, proceed to **Step 12**.
12. Press **Enter**. The system formats the diskette. When the formatting is complete, the system asks if you would like to format another diskette.
13. Type **N**.
14. Press **Enter**. The system begins copying the files.
15. When the system has finished copying the files, remove **Rescue Disk 2** and insert **Rescue Disk 3** into drive A.
16. Press **Enter**. The system displays a warning that the diskette will be formatted.
17. Press **Enter**. The system prompts you to insert a diskette. As you already have a diskette in drive A, proceed to **Step 18**.
18. Press **Enter**. The system formats the diskette. When the formatting is complete, the system asks if you would like to format another diskette.
19. Type **N**.
20. Press **Enter**. The system begins copying the files.
21. When the system has finished copying the files, remove **Rescue Disk 3** from drive A.
22. Set the write-protect tab on each diskette to prevent any modifications.

If necessary, you can run a Command AntiVirus scan from the rescue disk set.

Disk 1 contains the **FIXDISK** utility and the **RESCUE.DAT** file that contains a copy of the master boot record and boot sector.

As the rescue file on **Rescue Disk 1** is machine-specific, this diskette is for use only on the computer that was used to create the file.

You have just created a CSAV Rescue Disk set. Put the rescue disk set in a safe place. Be sure to update the set when you get your next Command AntiVirus update.

USING THE RESCUE DISK SET

The rescue disk process allows you to detect and remove any executable, boot sector, and MBR-infecting viruses that inhibit or prevent system startup. It then focuses on scanning and disinfecting all remaining virus-infected files, for example, macro virus-infected files.

To use the rescue disk set, follow these steps:

1. Turn off your computer.
2. Place a virus-free, write-protected bootable diskette into drive A.
3. Turn on your computer.
4. If you are prompted to enter a new date and a new time, press **Enter** for each.
5. Remove the bootable diskette and insert **Rescue Disk 1** into drive A.
6. At the A prompt, type the following:

```
F-PROT /HARD /DISINF /LOADDEF /ALL
```

7. Press **Enter**. The system prompts you to insert a diskette with **SIGN.DEF**.
8. Insert **Rescue Disk 2** into drive A and press **Enter**. The system prompts you to insert a diskette with **SIGN2.DEF**.

9. Insert **Rescue Disk 3** into drive A and press **Enter**. A scan of your hard drive begins immediately. If any viruses are detected, allow CSAV to disinfect them.
10. When the scan is complete, remove **Rescue Disk 3** from drive A.

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.

DOS

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 EXCHANGE

Command AntiVirus for Microsoft® Exchange is for use by experienced system administrators to prevent viruses from being transmitted through a Microsoft® Exchange Server network.

MAIN FEATURES

Command AntiVirus for Microsoft Exchange is a comprehensive antivirus protection program that:

- Automatically disinfects virus-infected e-mail attachments without damaging the attachment.
- Installs quickly and easily on your server.
- Performs on-access and on-demand scanning.
- Quarantines infected files for disinfection, examination or deletion.
- Generates multiple, detailed virus scanning statistics.
- Runs as a Windows service and provides event logging.
- Allows administrators to e-mail virus alert messages automatically.
- Automatically sends disinfected e-mail to its intended recipients.
- Provides a highly flexible scheduled scanning feature.
- Uses state-of-the-art scanning technology to detect thousands of known viruses and their variants.
- Uses easy to understand configuration options.
- Allows you to define and configure rules to manage infected items received by the Exchange Server.

SYSTEM REQUIREMENTS

To install and operate Command AntiVirus for Microsoft Exchange, your system must meet the following minimum requirements:

- Pentium CPU
- 96 MB of RAM (128 MB recommended)
- 30 MB of available hard disk space
- Microsoft® Windows® 2000 Advanced Server with Service Pack 2 or higher
- Microsoft® Exchange 2000 Server with Service Pack 1 or higher

NOTE: If you are experiencing difficulties with memory usage prior to installing the program, you may need to increase your server's memory to insure the proper operation of Command AntiVirus.

INSTALLATION

Installing CSAV is a very simple process. However, we recommend that you read the installation instructions prior to installing. This will help you make some of the setup choices during the installation procedure.

INSTALLING

NOTE: Before installing CSAV for Exchange, make sure that:

- Microsoft Exchange 2000 Server with SP1 or higher is running on your server.
- You are logged on as an administrator on the local domain.
- You remove any previous versions of Command AntiVirus for Exchange.
- You are **not** installing Command AntiVirus for Exchange through terminal services.

To install Command AntiVirus for Microsoft Exchange, follow these steps:

1. Insert the CD-ROM.
2. On the taskbar, click the **Start** button.
3. Click **Run**. The system displays the **Run** dialog box.
4. Select **Browse** to search the CD for the **EXCHANGE** directory.
5. Change to that directory.
6. Double-click **Setup.exe** and click **OK**. After startup, the system displays the **Welcome** dialog box.
7. Click **Next**. The system displays the **Software License Agreement**.
8. To accept the license agreement, click **Yes**. The system displays the **Setup Type** dialog box.
9. Select **one** of the following installations. We recommend the **Complete** installation.
    - **Complete –** Installs all required files.
    - **Custom –** Allows you to choose whether to install program files and help files.
10. Specify the **Destination Folder** for the CSAV for Exchange files. You can accept the default destination folder or click the **Browse** button to select a different folder.

11. Click **Next**. The system displays the **Select Service Start Options** dialog box.

NOTE: If you chose the **Custom** installation, the system first displays the **Select Features** dialog box. You can install either the Program Files or Help Files, or both. Select the features that you want to install and click **Next**.

This dialog box allows you to select which services to start. We recommend that you select **all** six of the options listed below. This is the default setting.

The **Scheduler** service allows you to schedule virus scans. The **SMTP Sink** service allows you to scan SMTP mail. SMTP mail includes mail that is sent over the Internet. The **Outbreak Manager** service allows you to define and configure rules to manage infected items received by the Exchange Server.

- Automatically start the CSAV for Exchange Scheduler service on system startup.
- Start CSAV for Exchange Scheduler service upon completion of installation.
- Start CSAV for Exchange SMTP Sink service upon completion of installation.
- Automatically start the CSAV for Exchange SMTP Sink service on system startup.
- Start the CSAV for Exchange Outbreak Manager service upon completion of installation.
- Automatically start the CSAV for Exchange Outbreak Manager service on system startup.

NOTE: The **On-access** service that provides real-time virus protection for your Exchange mail system is started automatically when the antivirus application programming interface (AVAPI) is loaded. The on-access service will **not** be listed in the Windows **Services** window.

12. Click **Next**. The system displays the **Start Copying Files** dialog box.

NOTE: If you want to review or change any settings, click **Back**.

13. Click **Next**. The installation program begins copying the CSAV for Exchange files to your system.

    When the copying is complete, the system displays the **CSAV for Exchange Options dialog** box.

14. Under the **Administrator Name** text box, use the **Browse** button to select a mail administrator for the Microsoft Exchange Server.

    When a virus-infected attachment is detected through the on-access scan task, by default CSAV sends a **mail alert message** to the mail administrator designated here.

    If you want to cancel sending a **mail alert message** to the Microsoft Exchange Server Administrator, clear the **Send alerts to administrator** check box.

NOTE: You can also start or cancel sending a **mail alert message** from the **CSAV for Exchange Console** menu bar by clicking **Tools**, and then clicking **Options**. For more information, refer to **Options** under **Using the Tools Menu** located in the ***Using Command AntiVirus*** chapter of the *Command AntiVirus for Exchange Administrator's Guide*.

15. Under **Quarantine Folder**, you can use the **Browse** button to change the Exchange mail folder that holds infected files in quarantine. The default is:

```
Program Files\Command Software\CSAV for Exchange\Quarantine.
```

    For more information on the quarantine feature, refer to **Using the Quarantine Feature** located in the ***Using Command AntiVirus*** chapter of the *Command AntiVirus for Exchange Administrator's Guide*.

16. After you have selected the **Administrator Name** and the **Quarantine Folder**, click **Next**. When the installation is complete, the system displays the **Setup Complete** dialog box.

17. Select whether you want to view the **README** file and/or run the **CSAV for Exchange console.** We recommend that you view the **README** file as it contains the latest information on the functionality of CSAV for Exchange.

18. Click **Finish**. This completes the installation of CSAV for Exchange.

GETTING STARTED

To start using Command AntiVirus for Exchange, follow these steps:

1. On the Windows taskbar, click the **Start** button.
2. Select **Programs**.
3. Select **Command Software**.
4. Select **CSAV for Exchange**.
5. Click the **CSAV for Exchange Console** icon. The system displays the **CSAV for Exchange Console**.

CSAV FOR EXCHANGE CONSOLE

CSAV uses a graphical user interface (GUI) that simplifies the customizing and starting of virus scans. When you start CSAV for Exchange, the program displays the **CSAV for Exchange console**.

From the **console**, you can perform numerous scan task operations. For example, you can create, start, modify, or delete virus scans. You can also change the folder in which detected viruses are quarantined. These scan task operations can be performed easily from the menu bar, the toolbar or through the command buttons. For more information, refer to the ***Using Command AntiVirus*** chapter of the *Command AntiVirus for Exchange Administrator's Guide*.

SCANNING FEATURES

Command AntiVirus for Exchange contains the following scanning features.

ON-ACCESS SCAN TASK

At startup, CSAV uses a default on-access (real-time) scan task. The on-access scan task runs continuously in the background monitoring incoming and outgoing e-mail. When an e-mail is sent or received by the Exchange Server, any attachments present in the e-mail are scanned automatically for infections. The on-access scan task is identified by the yellow **C** icon.

The CSAV on-access scan task scans only those mail boxes that are on the server where CSAV for Exchange is installed.

NOTE: CSAV can have only **one** on-access scan task. You cannot create a new on-access task or delete the existing one. However, you can enable, disable, and configure the on-access task to meet your needs.

Configuring the On-access Scan Task

To configure the on-access scan task, follow these steps:

1. In the **CSAV for Exchange console**, select the on-access task.
2. If the Status of the task is **Enabled**, continue to **Step 3**.

   If the **Status** of the task is **Disabled**, click **Task** on the menu bar and then click **Enable**.
3. Click the **Properties** button. The system displays the **Properties** dialog box that contains the **Detection**, **Actions**, **Advanced**, and **Reports** dialog boxes.
4. In each dialog box, specify the options that meet your requirements. For more information on configuring scan task properties, see **Configuring Scanning Properties** in the ***Using Command AntiVirus*** chapter of the *Command AntiVirus for Microsoft Exchange Administrator’s Guide.*
5. Click **OK**.

ON-DEMAND SCAN TASKS

On-demand scan tasks scan e-mail attachments within folders and mailboxes upon request. You can start an on-demand scan immediately or periodically at a specific time. Also, you can create multiple on-demand scan tasks and configure each one to meet your needs. For example, you can create on-demand scan tasks that can scan all or just some of the Exchange Server information store.

Creating and Configuring On-demand Scan Tasks

To create an on-demand task, follow these steps:

1. On the menu bar, click **Task**. The system displays the **Task** menu.
2. Click **New Task**.
3. Give the new task a name and press **Enter**.
4. Click the **Properties** button. The system displays the **Properties** dialog box that contains the **Detection**, **Actions**, **Advanced**, **Reports**, **Schedule**, and **Exclusion** dialog boxes.
5. In each dialog box, specify the options that meet your requirements. For more information on configuring scan task properties, see **Configuring Scanning Properties** in the ***Using Command AntiVirus*** chapter of the *Command AntiVirus for Microsoft Exchange Administrator's Guide.*
6. Click **OK**.

QUARANTINE FEATURE

The quarantine feature allows administrators to move infected attachments to a secure location for evaluation, disinfection, or deletion at a later time.

When an attachment is quarantined, the original attachment is replaced by a new attachment that contains a description of where the virus was found.

By default, the file name of the new attachment contains the original file name with the extension **.VIRUS INFO.TXT** added to it. For more information, see **Using the Quarantine Feature** in the ***Using Command AntiVirus*** chapter of the *Command AntiVirus for Microsoft Exchange Administrator's Guide.*

NOTE: When an infected file is moved, it is renamed. The new name contains the original file name and extension, the name of the virus with a maximum of 30 characters, and a **VIRUS** extension. If the file name already exists in the **Quarantine** folder, a random number is added to the end of the **VIRUS** extension. If the name is still not unique, another random number is added.

Specifying the Quarantine Folder

Before you can use the quarantine feature, you **must** specify a quarantine folder.

To specify a quarantine folder, follow these steps:

1. In the **CSAV for Exchange console**, on the menu bar, click **Tools**. The system displays the **Tools** menu.
2. Click **Options**. The system displays the **CSAV for Exchange Options** dialog box.
3. Specify the following:

   - **Administrator Name –** Use the **Browse** button to select an administrator for the Microsoft Exchange Server from the **Choose Administrator(s)** dialog box. This mailbox is used to send MAPI alert messages when a virus-infected attachment is detected through the on-access scan task.

NOTE: Your selection replaces the mail administrator that you specified during the installation.

NOTE: If you do **not** want a **mail alert message** sent to the Exchange Server Administrator, clear the **Send alerts to administrator** check box.

   - **Quarantine Folder** – Use the **Browse** button to select a quarantine folder from the **Browse For Folder** dialog box.

4. Click **OK**.

Specifying the Quarantine Log File Size

The default size of the quarantine log file is 100 KB. The minimum log file size is 10 KB. The maximum size is 999 KB. To specify a custom log file size, do the following:

1. On the menu bar, click the **Task**. The system displays the **Task** menu.
2. Click **Properties**. The system displays the **Properties** dialog box.
3. Select the **Reports** tab. In the **Log file** pane, select the **Limit size of log file to** check box. You can enter a custom size by typing a new size into the **kilobytes** text box or by using the up and down arrows on the text box.
4. Click **OK**.

Moving Files to the Quarantine Folder

Infected files are moved to the **Quarantine** folder when the **Quarantine infected items automatically** option is selected in the **Actions** dialog box.

To enable this option for a specific scan task, follow these steps:

1. In the **CSAV for Exchange console**, select a task from the **Task List**.
2. On the menu bar, click **Task**. The system displays the **Task** menu.
3. Click **Properties**. The system displays the **Properties** dialog box.
4. Click the **Actions** tab. The system displays the **Actions** dialog box.
5. In the **When a virus is found** group box, click the down arrow and select **Quarantine infected items automatically**.
6. Click **OK**.

NOTE: Remember, this option must be configured for each scan task.

You can also move infected files to the **Quarantine** folder by selecting the **If specified action fails Quarantine attachment** option in the **Actions** dialog box. For more information, see **Action to Take On Infection** in the ***Using Command AntiVirus*** chapter of the *Command AntiVirus for Microsoft Exchange Administrator's Guide.*

VIRUS NOTIFICATION

If a virus-infected attachment is detected through the on-access scan task, by default CSAV sends a **mail alert message** to the sender, the intended recipients, and the mail administrator designated at the time of the CSAV for Exchange installation.

You can send a mail alert message to additional administrators, change the text of the message that is sent, and cancel sending an alert to the additional administrators. To configure these options, on the **CSAV for Exchange Console** menu bar, click **Tools**, and then click **Notification**.

NOTE: This option does **not** change the Microsoft Exchange Server Administrator that you specified during the installation, or cancel sending an alert to the Microsoft Exchange Server Administrator. To configure these options, on the **CSAV for Exchange Console** menu bar, click **Tools**, and then click **Options**. For more information, see **Options** in the ***Using Command AntiVirus*** chapter of the *Command AntiVirus for Microsoft Exchange Administrator's Guide.*

Notifications are **not** sent if a virus is detected through an on-demand scan.

For more information, see **Virus Notification** in the ***Using Command AntiVirus*** chapter of the *Command AntiVirus for Microsoft Exchange Administrator's Guide.*

OUTBREAK MANAGER

The Outbreak Manager allows you to define and configure rules to manage infected items received by the Exchange Server. Enabling this option allows you to:

- **Configure Rules** specific to your environment.
- Define **Outbreak Conditions** for each configured rule.
- Define the **Outbreak Actions** to be taken for each defined condition.
- Set up a log file using **Settings**. You can specify the file path and file size.
- View the log file using **View log**.

To set up **Configuration Rules**, **Outbreak Conditions**, and **Outbreak Actions**, follow these steps:

1. On the menu bar, click **Tools**. The system displays the **Tools** menu.
2. Click **Outbreak Manager,** and then click **Configuration Rules**. The system displays the **CSAV Outbreak Rules** dialog box.
3. Click **New.** The system displays the **CSAV Outbreak Conditions** dialog box.
4. Select a condition, and specify the parameters to be used with the condition.
5. Click **Next.** The system displays the **CSAV Outbreak Actions** dialog box.
6. Select at least one action to be taken when the defined condition is encountered, and define the values associated with the specified action(s).
7. Click **Next.** The system displays the **CSAV Options** dialog box.
8. Name the configuration rule, and select a **Mode of action**.
9. Click **Next.** The system displays the **CSAV Outbreak Summary** dialog box describing the new rule.
10. Click **Finish**.The system displays the **CSAV Outbreak Rules** dialog box with the new configuration rules listed.
11. Click **Apply**, and then click **OK**.

To set up a log file for **Outbreak Manager**, follow these steps:

1. On the menu bar, click **Tools**. The system displays the **Tools** menu.
2. Click **Outbreak Manager,** and then click **Settings**. The system displays the **Outbreak Manager Settings** dialog box.
3. Under **Log Details**, in the **File Path** text box, specify the path to the log file. The default is `C:\Program Files\Command Software\CSAV For Exhange\CSOutbreakMgr.log`. To change the path, click the **Browse** button.
4. Under **Log Details**, in the **File Size (mb)** text box, specify the log file size. The default log file size is 20 MB.
5. Under **Settings**, you can specify if you do not want the **Outbreak Manager** icon to appear in your system tray. If you do not want the icon to appear in the system tray, clear the **Show CSAV For Exchange Outbreak Manager Icon on Taskbar** checkbox.

To view the log file for **Outbreak Manager**, follow these steps:

1. On the menu bar, click **Tools**. The system displays the **Tools** menu.
2. Click **Outbreak Manager**, and then click **View log.** The system displays the **CSOutbreakMgr.log** file.

For more information about Outbreak Manager, refer to **Outbreak Manager** in the ***Using Command AntiVirus*** chapter of the *Command AntiVirus for Microsoft Exchange Administrator's Guide*.

VIRUS SCANNING RESULTS

Command AntiVirus for Exchange provides several ways to get information about on-access and on-demand scans.

VIEWING SCAN STATISTICS

The **Statistics** dialog box displays the results of a scan as well as the number of files that were scanned.

To view the statistics for a scan task, follow these steps:

1. In the **CSAV for Exchange console**, select a task from the **Task List**.
2. On the menu bar, click **Task**. The system displays the **Task** menu.
3. Click **Statistics**. The system displays the **Statistics** dialog box.

USING EVENT VIEWER TO VIEW SCAN RESULTS

The Windows operating system has a built-in viewer that allows you to monitor the status of various system-related events. This viewer is called **Event Viewer**. From within **Event Viewer**, you can view which CSAV events were started or ended. You can also view scan results such as the number of files scanned, infected, disinfected, deleted, and moved.

To view scan statistics and other CSAV-related events, follow these steps:

1. On the menu bar, click **Tools**. The system displays the drop-down menu.
2. Click **Event Viewer**.
3. In the **Event Viewer Tree**, select **Application Log**. The system displays the log of events in the right pane.

NOTE: You can also access Event Viewer by clicking the **Event Viewer** button on the toolbar.

VIEWING THE ACTIVITY LOG FILE

The **Activity Log** contains information on the number of files scanned, found, disinfected, deleted, and quarantined. It also has information on the status of many CSAV functions.

To view a task's **Activity Log**, follow these steps:

1. In the **CSAV for Exchange console**, right-click the task's name in the **Task List**. The system displays the shortcut menu.
2. Click **View Log**. The system displays the **Activity Log**.

AUTOMATIC UPDATE

The **Automatic Update** feature provides the easiest and most efficient method available for keeping the latest version of CSAV for Exchange running on your system. After you have configured the automatic update feature, Command AntiVirus for Microsoft Exchange can update itself with the latest program and virus definition files. Thus, the automatic update feature assures you that your Exchange mail system is always being protected by the latest antivirus technology.

For complete instructions on how to configure the **Automatic Update** feature, see the ***Automatic Update*** chapter in the *Command AntiVirus for Microsoft Exchange Administrator's Guide.*

TRAP NOTIFICATIONS

When CSAV for Exchange generates traps, notifications can be sent to other computers using Simple Network Management Protocol (SNMP). SNMP must be installed and enabled on your Windows 2000 Server before trap notifications can be sent.

To view trap notifications, you must have a network management system, such as Castle Rock SNMPc Network Manager or Hewlett Packard OpenView, installed on the systems receiving trap notifications.

To send notifications of traps generated by CSAV for Exchange, follow these steps:

1. On the menu bar, click **Tools**. The system displays the **Tools** menu.
2. Click **CSAV Alerts**. The system displays the **CSAV Alerts** dialog box.
3. Select the **Enable SNMP Trap** check box.
4. In the **components** pane, select one or more of the components.
5. Click **OK**.

REMOVING COMMAND ANTIVIRUS

To remove Command AntiVirus for Microsoft Exchange, follow these directions.

1. On the Windows taskbar, click the **Start** button.
2. Select **Settings**.
3. Click **Control Panel**.
4. Double-click the **Add/Remove Programs** icon.
5. Select **CSAV for Exchange** from the list of installed applications.
6. Click the **Change/Remove** button. The uninstall wizard prepares for the uninstall and the system displays a message box asking if you want to completely remove CSAV for Exchange and all its features.
7. Click **Yes**. When the uninstall completes, the system displays the **Maintenance Complete** dialog box.
8. To restart your computer now, select **Yes, I want to restart my computer now**, and click **Finish**. To restart your computer at a later time, select **No, I will restart my computer later**, and click **Finish**.

⚠ A system restart is required to completely remove CSAV for Exchange.

CSAV FOR NETWARE

SYSTEM REQUIREMENTS

To operate Command AntiVirus for NetWare, you need an IBM-compatible server with 16 MB of RAM above and beyond the minimum amount of RAM recommended for running Novell® NetWare

Command AntiVirus for NetWare protects Novell NetWare 4.x, 5.x, and 6.0. Command AntiVirus for NetWare runs independently of both bindery and NDS.

NetWare Client32 is required to run the Command AntiVirus for NetWare Administration program. Command AntiVirus for NetWare Administration is compatible with Microsoft® Windows® 95, Windows® 98, Windows® Me, Windows NT®, Windows® 2000, and Windows® XP.

NOTE: As Command AntiVirus for NetWare Administration is now a 32-bit application, this program does **not** run on Windows® 3.x.

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.EXE** from Windows at a workstation allows you to install the NLMs to the server. It also allows you to install the Command AntiVirus for NetWare Administration program, which runs on Windows, to the server or to a workstation.

1. Insert the CD into the CD-ROM drive on a workstation.
2. From the workstation, log on to the server with an ID that has full rights to **SYS:\SYSTEM** and to the directory where Command AntiVirus for NetWare Administration is to be placed. This allows the installation routine to create subdirectories and copy files to the correct locations.
3. Click the **Start** button and then **Run**.
4. Select **Browse** to search the CD for the **NETWARE** 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 for NetWare 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.

✓ **NOTE:** You **must** be logged on to each server that you select.

When you select a server, Setup creates a subdirectory called **F-PROT** under **SYS:\SYSTEM**. Setup then copies most of the Command AntiVirus files to this new directory: **SYS:\SYSTEM\F-PROT**. The remaining seven (7) files are copied to **SYS:\SYSTEM**. These files are:

- FPNCON.NLM
- F-DELAY.NLM
- F-PROT.NLM
- TTCONFIG.NLM
- VSENGINE.NLM
- CSAV-RMA.NLM
- CSAVHTTP.NLM

Click **OK** to continue.

12. After installing some files, Setup displays the first of a series of information dialog boxes. Read the information contained in each box and click **OK** to continue.
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: 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 can also be used if the INI file has been deleted or moved.

CONSOLE INSTALL

This procedure does not install the Windows-based 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 **NETWARE** 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 “-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: 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.

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.

Command AntiVirus contains file types that are scanned by default. These file types are displayed in the **Include List** dialog box of either the **Manual Scans** or **Real-time** menu items on the **Task** menu.

NOTE: Although Command AntiVirus scans certain file types by default, it does **not** scan self-extracting files. Dynamic Virus Protection (DVP) scans the contents of the self-extracting file when the files are extracted. However, the .EXE portion of the self-extracting file is scanned by default.

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 **CSAV** 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 Command AntiVirus for NetWare 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 real-time, manual and scheduled scans. The **Task** menu also lets you create new scanning tasks.

Deploy Menu

The **Deploy** menu provides the ability to send 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

The **View** menu allows you to see the Command AntiVirus log. 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.

Setup Menu

The **Setup** menu allows you to change passwords and manage the CSAV domain.

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.

Help Menu

The **Help** Menu allows you to locate information on topics of interest including instruction on how to use the features found in CSAV for NetWare Administration.

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.*

NOTE: For the deployment and updating processes of Command AntiVirus to work properly, the IPX-SPX services on NetWare servers **must** be enabled.

UPDATING THE DEFINITION FILES

This section contains information on updating the virus definition files (deffiles) automatically to a single server or manually from a workstation to a central location on each server.

The automated process allows you to automatically download and update the deffiles on a single server. You can then deploy the update to additional servers.

The manual process allows you to update the virus definition files (deffiles) from a workstation to a central location on each server. This eliminates the need to manually unload **F-PROT**, copy the updated files to the **F-PROT** directory, and reload **F-PROT** at each server.

AUTOMATICALLY

NOTE: For the automatic update to work, you **must** be able to connect to the Internet.

To automatically update the deffiles on a single server, follow these steps:

1. In the **SYS:\CSAVNDEF** directory on the server that you are updating, create a file called **csavupdt.ini**.
2. In the **csavupdt.ini** file, type the following:

```
server=download.commandsoftware.com
username=user
password=password
```

NOTE: **User** represents your Command user name. **Password** represents your Command password. You **must** use a valid user name and password.

NOTE: As the IP address of the downloads may change, to prevent failure of future updates, we highly recommend that you enable DNS on the file server.

If you do **not** have DNS enabled, you **must** check the Frequently Asked Questions (FAQ) section of our web site for the **current IP** address — www.commandsoftware.com/service/support/FAQSearch.asp.

Just search the **CSS ANSWERBOOK** by typing **one** of the following options in the **SEARCH TEXT** box and clicking **SEARCH**:

021111

IP address

3. Save the file.

4. To start the program, type:

```
LOAD CSAVHTTP
```

NOTE: If you want the program to start automatically after you restart the server, add the **LOAD CSAVHTTP** command to the **AUTOEXEC.NCF** file.

If the definition files are out of date, the updated deffile update called **DEFFILES.EXE** is downloaded from our web and extracted. Then, the following extracted files are copied to the **SYS:\CSAVNDEF** directory on the server that you are updating:

- SIGN.DEF
- SIGN2.DEF
- MACRO.DEF

NOTE: **DEFFILES.EXE** contains five (5) files. NetWare does **not** use the **NOMACRO.DEF** or **CSS_1740.CSV** files.

NOTE: Command AntiVirus for NetWare checks the **SYS:\CSAVNDEF** directory for updated deffiles approximately every hour. After you install Command AntiVirus for NetWare, it automatically creates the **CSAVNDEF** directory the first time it checks for updated deffiles. If the directory does not exist and you do not want to wait, you can create this directory.

If deffiles are present in the **SYS:\CSAVNDEF** directory, virus scanning is temporarily suspended while Command AntiVirus copies the deffiles to the **SYS:\SYSTEM\F-PROT** directory. Virus scanning resumes after the deffiles are copied.

NOTE: When Command AntiVirus copies the deffiles to the **SYS:\SYSTEM\F-PROT** directory, it renames the old deffiles with a **.OLD** extension. If there are any problems with the new deffiles, Command AntiVirus uses the old deffiles by renaming them to their original names. The following error message is displayed at the server console:

```
F-PROT: mm/dd/yyyy hh:mm:ss ERROR INITIALIZING THE SCAN ENGINE:
ERROR IN DEF FILES ROLLING BACK!
```

NOTE: The mm/dd/yyyy represents the month, day and year. The hh:mm:ss represents the time in hours, minutes and seconds.

Command AntiVirus deletes the new deffiles from the **SYS:\CSAVNDEF** directory after they are copied to the **SYS:\SYSTEM\F-PROT** directory.

MANUALLY

To update the deffiles to a central location on a server, follow these steps:

1. Download the deffile update file called **DEFFILES.EXE** from our web site to a temporary directory.
2. Go to the temporary directory containing **DEFFILES.EXE**, and double-click the file to extract the files that are contained within it.

3. Copy the following extracted files to the **SYS:\CSAVNDEF** directory on the server that you are updating:

   - SIGN.DEF
   - SIGN2.DEF
   - MACRO.DEF

NOTE: **DEFFILES.EXE** contains five (5) files. NetWare does **not** use the **NOMACRO.DEF** or **CSS_1740.CSV** files.

NOTE: Command AntiVirus for NetWare checks the **SYS:\CSAVNDEF** directory for updated deffiles approximately every hour. After you install Command AntiVirus for NetWare, it automatically creates the **CSAVNDEF** directory the first time it checks for updated deffiles. If the directory does not exist and you do not want to wait, you can create this directory.

If deffiles are present in the **SYS:\CSAVNDEF** directory, virus scanning is temporarily suspended while Command AntiVirus copies the deffiles to the **SYS:\SYSTEM\F-PROT** directory. Virus scanning resumes after the deffiles are copied.

NOTE: When Command AntiVirus copies the deffiles to the **SYS:\SYSTEM\F-PROT** directory, it renames the old deffiles with a **.OLD** extension. If there are any problems with the new deffiles, Command AntiVirus uses the old deffiles by renaming them to their original names. The following error message is displayed at the server console:

```
F-PROT: mm/dd/yyyy hh:mm:ss ERROR INITIALIZING THE SCAN ENGINE:
ERROR IN DEF FILES ROLLING BACK!
```

NOTE: The mm/dd/yyyy represents the month, day and year. The hh:mm:ss represents the time in hours, minutes and seconds.

Command AntiVirus deletes the new deffiles from the **SYS:\CSAVNDEF** directory after they are copied to the **SYS:\SYSTEM\F-PROT** directory.

REMOVING COMMAND ANTIVIRUS

You can remove Command AntiVirus for NetWare by using the **DEINSTALL** command. This can be done only 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 **CSAV 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 DEIN-
   STALLED.
   ```

3. You will be prompted to enter a password. This is the same password you selected in Command AntiVirus for NetWare 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. You should review these changes to insure proper operation.

NOTE: If you have installed Command AntiVirus client files on your workstation, you should also:

1. Manually delete the **F-PROT** directory from the hard drive.
2. Manually delete the **FPNADMIN.INI** file from the Windows directory.