Command AntiVirus™

for

Windows NT®/2000

Administrator’s Guide

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. C2000-460-0101**

Part No. 07-0501-00A

TABLE OF CONTENTS

INTRODUCTION

Congratulations on choosing Command AntiVirus for Windows NT®/2000 for unsurpassed security against computer viruses! Command AntiVirus provides you with the latest technology for preventing the spread of computer viruses.

MAIN FEATURES

Command AntiVirus (CSAV) for Windows NT/2000 is a comprehensive anti-virus protection program that:

- Windows NT compliance includes a 32-bit scanner and a kernel-mode driver with support for long file names and Universal Naming Convention (UNC) path names.
- A service that allows scheduled scans to run in the background on local drives.
- Right mouse support allows you to easily start a scan on any file or folder.
- Installation is an easy one-step process.
- On-access scanning of files and disks by the kernel-mode driver as they are accessed.
- Separate administrative and user-defined tasks.
- Automatic isolation of virus infections to a quarantine folder.
- Administrator can create tasks that cannot be modified by users.
- Complete scheduling assigns scans to a specific day, week, month or after periods of inactivity.
- Fully configurable inclusion/exclusion of files and folders from the scan list.

- Scans compressed files and compressed executables.
- Safely removes viruses from files, boot sectors and partition tables.
- Enterprise-wide messaging capabilities include electronic mail.
- Companion product notification (Command AntiVirus for NetWare).
- ICSA certified for effective virus protection.

CHAPTER OVERVIEW

The *Command AntiVirus for Windows NT®/2000 Administrator's Guide* consists of the following chapters:

CHAPTER 1 - INTRODUCTION

This chapter provides an overview of the product including a list of features, conventions and system requirements. Chapter 1 also contains details on accessing additional product-related information from the Command Software Systems web site.

CHAPTER 2 - INSTALLATION

Chapter 2 contains instructions on installing Command AntiVirus. This chapter also provides details on creating a rescue disk set, adding and removing features, and reinstalling and removing Command AntiVirus.

CHAPTER 3 - USING COMMAND ANTIVIRUS

This chapter provides information on configuring and using the features of Command AntiVirus.

For example, Chapter 3 includes details on creating, customizing, scheduling, and executing virus scan tasks. It also contains information on viewing scan results, customizing on-access scanning, and updating the virus definition files.

CHAPTER 4 - BOOT RECORD SUPPORT

Chapter 4 contains information on using our FIXDISK and FIXDSKNT utilities to remove unknown boot sector viruses. This chapter also provides details on the actions to take if you have difficulty disinfecting a boot sector virus.

CHAPTER 5 - DOS RECOVERY

This chapter provides information on the Command AntiVirus menu and command-line options that can be used in the DOS environment.

CHAPTER 6 - NETWORK ADMINISTRATION

Chapter 6 contains network administration techniques for installing, upgrading and operating Command AntiVirus.

For example, this chapter includes details on customizing your scan tasks, updates information, and installation settings. You can also find information on deploying Command AntiVirus to individual computers from a central location on a network.

CHAPTER 7 - CSS CENTRAL

This chapter covers the interface for distributing, updating, and modifying Command AntiVirus from a single location.

CHAPTER 8 - GLOSSARY

The ***Glossary*** provides definitions of virus terminology.

APPENDIX

The ***Appendix*** contains a list of Event ID messages that may be logged to the Windows **Event Viewer Application Log**.

CONVENTIONS USED

⚠	Indicates an area that requires special attention.
✓	Indicates a helpful tip.
	Indicates network-specific information.
	Indicates a task that requires administrator rights to perform.
SERVER	Indicates information that is specific to the server version of Command AntiVirus.
`COURIER`	Examples and messages appear in `COURIER`. For example: `C:\F-PROT\F-PROT /HARD /DISINF`
CSAV	The acronym used for Command AntiVirus

SYSTEM REQUIREMENTS

To install and operate Command AntiVirus for Windows NT/2000, you must have Windows 2000 installed.

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 know 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 United Kingdom at **www.command.co.uk**.

HELP FILES

The Help files contain information that will assist you in using the product.

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 Satisfaction or visit our web site.

README.TXT

The latest information on product enhancements, fixes and special instructions is in the README.TXT file that is included with the CSAV program files. You can also review this file on the Command Software Systems web site before you download the CSAV files.

INSTALLATION

INSTALLING

This section provides instructions on installing Command AntiVirus for Windows NT®/2000 on a single workstation or server. We suggest that you read through these instructions prior to installing the product. This will allow you to better anticipate any choices that you may need to make during the installation process.

During the installation, you will have the opportunity to choose a **Typical** or a **Custom** installation.

A **Typical** installation installs all of the components that are required for complete anti-virus protection. This option is selected by default.

A **Custom** installation allows you to select the components that you want to install.

For more information on administrative installation, customizing your installation settings and deploying to multiple users over the network, refer to the ***Network Administration*** chapter.

NOTE: To install Command AntiVirus, **one** of the following conditions **must** be met:

- You are a member of the local Administrators group
- System policy is set so that you have elevated privileges for installations
- Command AntiVirus has been advertised for all users
- Command AntiVirus has been assigned through Group Policy

To create a rescue disk set, you **must** be a member of the local Administrators group.

NOTE: To create a rescue disk set, you will need three blank, formatted 1.44 MB 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)**.

For NTFS systems, unless you can access an NTFS drive from within DOS, for example, by using third-party software, you will **not** be able to use the rescue disk set to scan files on an NTFS drive.

You can use **Rescue Disk 1** on NTFS systems at any time to repair damaged or infected boot sector information.

NOTE: Before running the installation program, we strongly recommend that you exit all Windows programs.

TYPICAL INSTALLATION

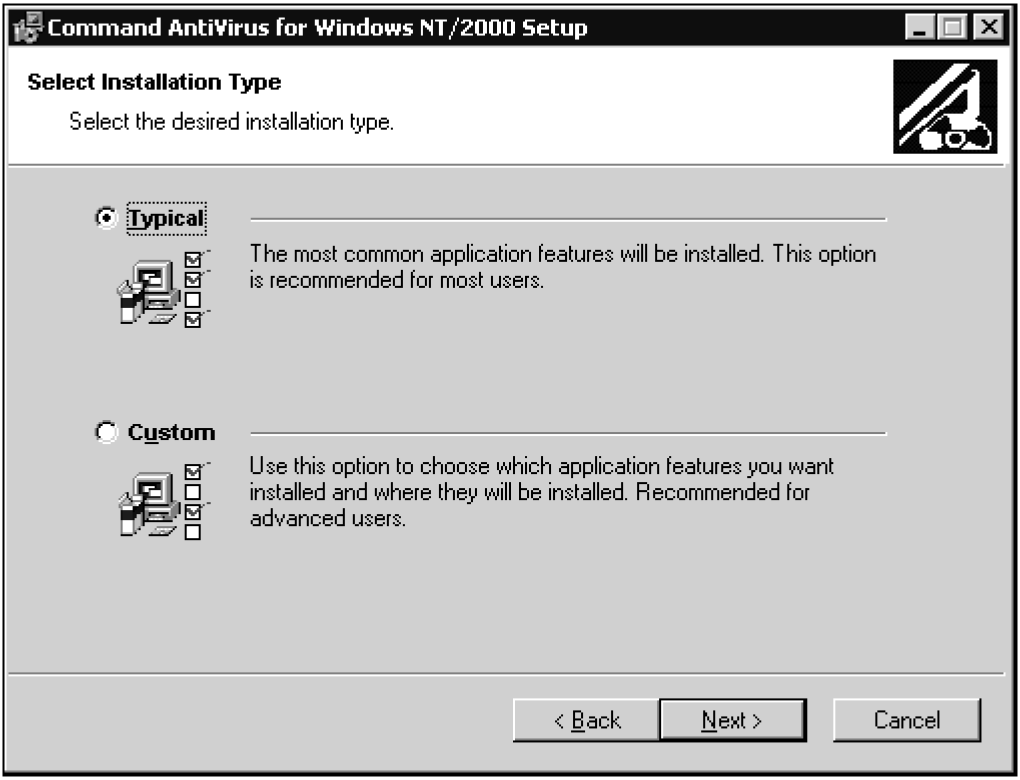
To install Command AntiVirus, follow these steps:

1. Insert the CD-ROM.
2. Click the **Start** button on the Windows task bar.
3. Click **Run**.
4. Click **Browse** to search the CD for the **WIN2000W** folder.

Click **Browse** to search the CD for the **WIN2000S** folder.

5. Open that folder.
6. Double-click **SETUP.EXE**. The system returns to the **Run** dialog box.

7. Click **OK**. The system displays the **Welcome** dialog box.
8. Click **Next**. The system displays the **License Agreement**.
9. To accept the license agreement, select **I accept the License Agreement** and click **Next**. The system displays the **Select Installation Type** dialog box:



Command AntiVirus for Windows NT/2000 Setup

Select Installation Type

Select the desired installation type.

● Typical

The most common application features will be installed. This option is recommended for most users.

○ Custom

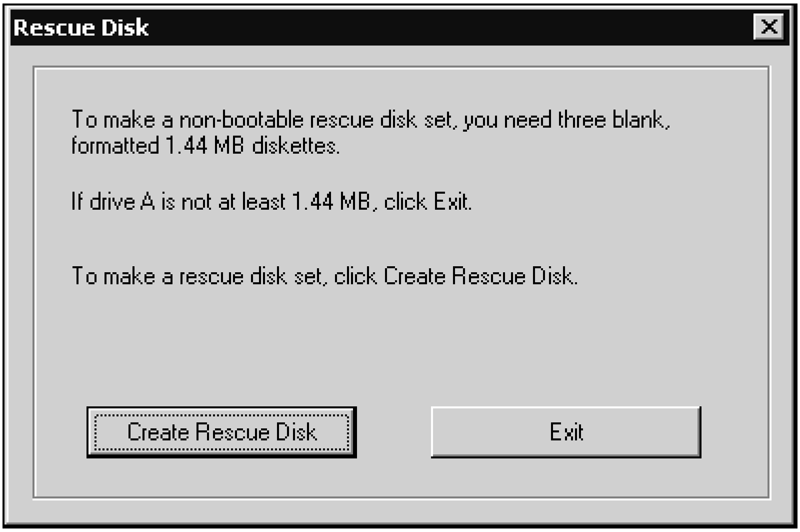
Use this option to choose which application features you want installed and where they will be installed. Recommended for advanced users.

Select Installation Type Dialog Box

10. Select **Typical** and click **Next**. The system displays the **Updating System** dialog box. Please wait while the program copies the Command AntiVirus files to your system.

NOTE: You can click **Cancel**, **Exit Setup** and then **OK** to cancel the installation and exit the setup program.

When the copying is complete, the system displays the **Rescue Disk** dialog box:



Rescue Disk

To make a non-bootable rescue disk set, you need three blank, formatted 1.44 MB diskettes.

If drive A is not at least 1.44 MB, click Exit.

To make a rescue disk set, click Create Rescue Disk.

Rescue Disk Dialog Box

To create a rescue disk set, you **must** be a member of the local Administrators group.

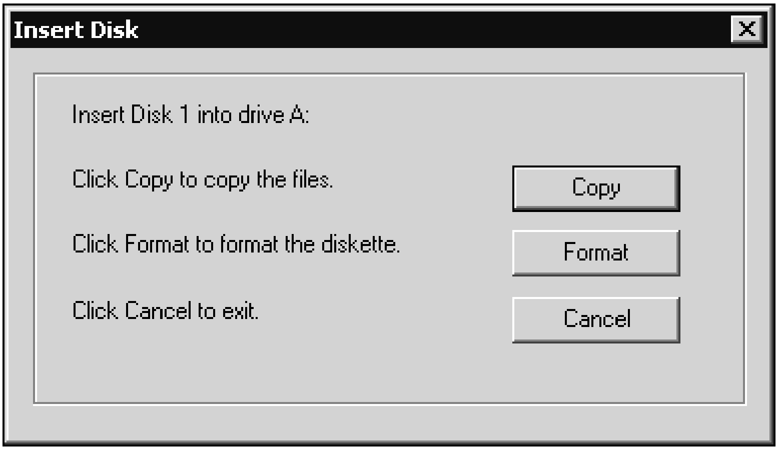
NOTE: To create a rescue disk set, you will need three blank, formatted 1.44 MB diskettes labeled **CSAV Rescue Disk 1 for (User's Computer ID)**, **CSAV Rescue Disk 2 for (User's Computer ID)**, and **CSAV Rescue Disk 3 for (User's Computer ID)**.

For NTFS systems, unless you can access an NTFS drive from within DOS, for example, by using third-party software, you will **not** be able to use the rescue disk set to scan files on an NTFS drive.

You can use **Rescue Disk 1** on NTFS systems at any time to repair damaged or infected boot sector information.

NOTE: If drive A is not at least 1.44 MB or you do not want to create a rescue disk set, click **Exit**.

11. To make a non-bootable rescue disk set, click **Create Rescue Disk**. The system displays the **Insert Disk** dialog box:



Insert Disk 1 into drive A:

Click Copy to copy the files.

Click Format to format the diskette.

Click Cancel to exit.

Insert Disk Dialog Box

12. Insert **Disk 1** into drive A and click **Copy**. The system returns to the **Rescue Disk** dialog box which displays the files being copied.

    To format a diskette, click **Format**. Then, continue with the formatting process. When the formatting process is complete, click **Close** to return to the **Insert Disk** dialog box.

13. When the copying is complete, the system displays a dialog box informing you that the rescue disk was created successfully. Click **OK** to continue. The system displays the **Insert Disk** dialog box.

14. Remove **Disk 1** from drive A, and set the write-protect tab to prevent any modifications.

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

15. Insert **Disk 2** into drive A and click **Copy**. The system returns to the **Rescue Disk** dialog box which displays the files being copied.

16. When the copying is complete, the system displays a dialog box informing you that the rescue disk was created successfully. Click **OK** to continue. The system returns to the **Rescue Disk** dialog box.

17. Remove **Disk 2** from drive A, and set the write-protect tab to prevent any modifications.

18. Insert **Disk 3** into drive A and click **Copy.** The system returns to the **Rescue Disk** dialog box which displays the files being copied.

19. When the copying is complete, the system displays a dialog box informing you that the rescue disk was created successfully. Click **OK** to continue. The system returns to the **Rescue Disk** dialog box.

20. Remove **Disk 3** from drive A, and set the write-protect tab to prevent any modifications.

21. Click **Exit**. The system displays a dialog box informing you that Command AntiVirus for Windows NT/2000 has been successfully installed.

22. Click **Finish** to exit.

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

CUSTOM INSTALLATION

To install Command AntiVirus, follow these steps:

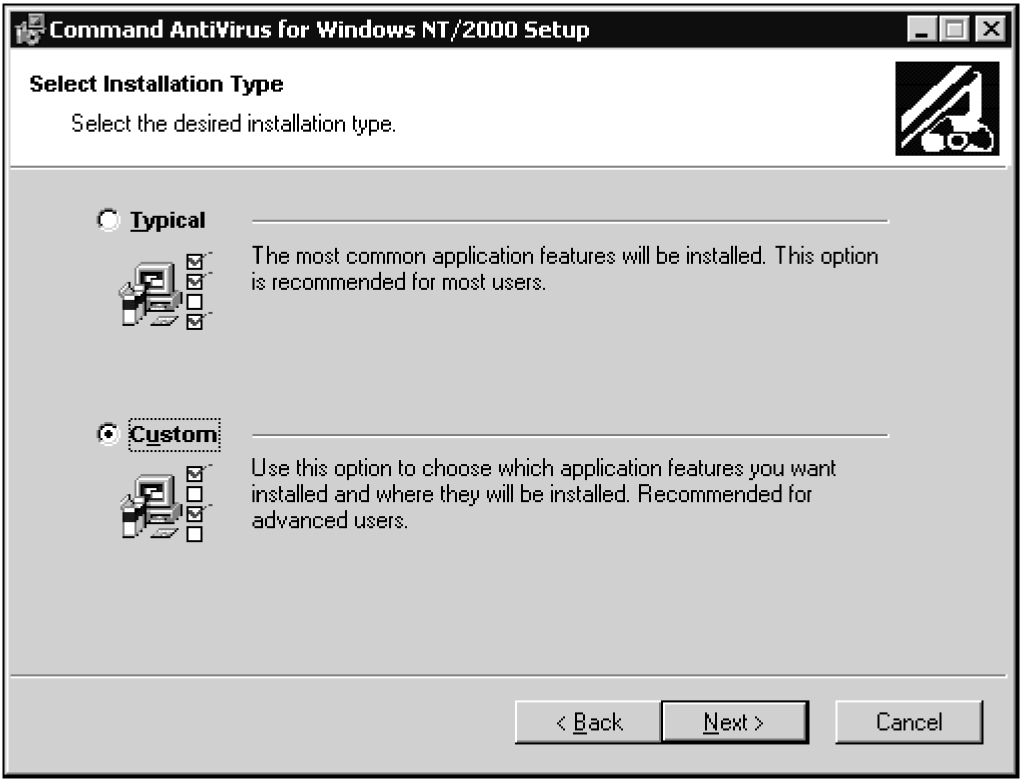
1. Insert the CD-ROM.
2. Click the **Start** button on the Windows task bar.
3. Click **Run**.
4. Click **Browse** to search the CD for the **WIN2000W** folder.

SERVER

Click **Browse** to search the CD for the **WIN2000S** folder.

5. Open that folder.
6. Double-click **SETUP.EXE**. The system returns to the **Run** dialog box.

7. Click **OK**. The system displays the **Welcome** dialog box.
8. Click **Next**. The system displays the **License Agreement**.
9. To accept the license agreement, select **I accept the License Agreement** and click **Next**. The system displays the **Select Installation Type** dialog box:



Command AntiVirus for Windows NT/2000 Setup

Select Installation Type

Select the desired installation type.

○ Typical

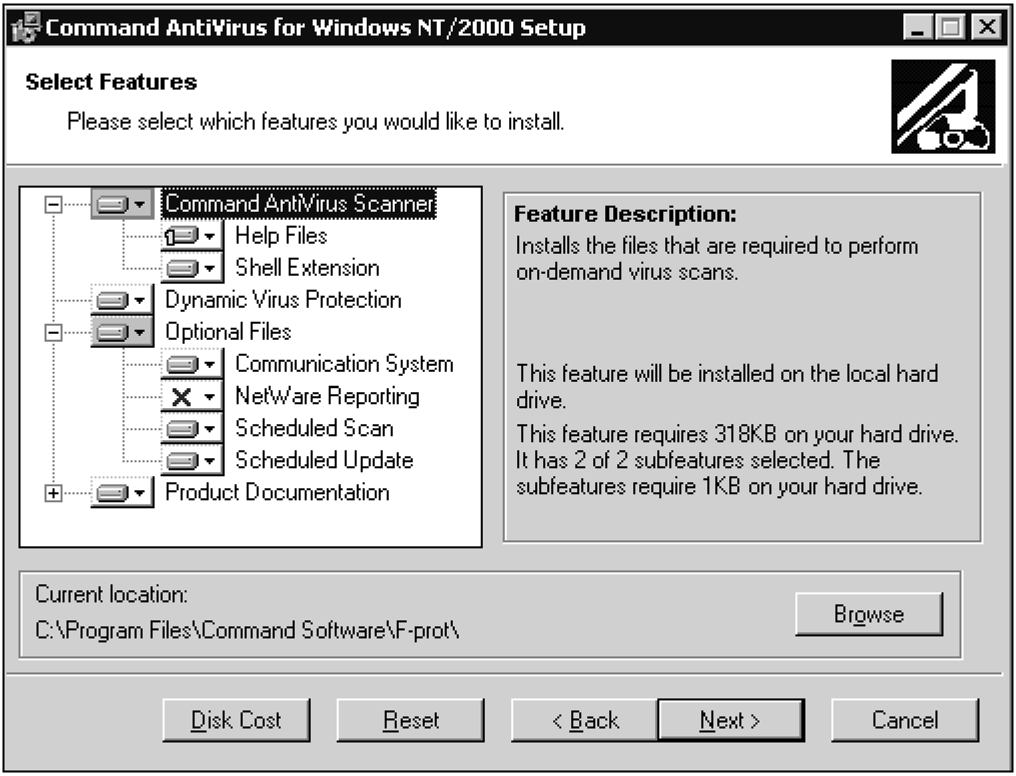
The most common application features will be installed. This option is recommended for most users.

● Custom

Use this option to choose which application features you want installed and where they will be installed. Recommended for advanced users.

Select Installation Type Dialog Box

10. Select **Custom** and click **Next**. The system displays the **Select Features** dialog box:


Command AntiVirus for Windows NT/2000 Setup

Select Features

Please select which features you would like to install.

- Command AntiVirus Scanner
  - Help Files
  - Shell Extension
- Dynamic Virus Protection
- Optional Files
  - Communication System
  - NetWare Reporting
  - Scheduled Scan
  - Scheduled Update
- Product Documentation

Feature Description:
Installs the files that are required to perform on-demand virus scans.

This feature will be installed on the local hard drive.

This feature requires 318KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 1KB on your hard drive.

Current location:
C:\Program Files\Command Software\F-prot\

Select Features Dialog Box

11. Select the features and subfeatures that you want to install. Click the plus signs (+) to display the subfeatures. You can view the description of each feature and subfeature by clicking its name.

- **Command AntiVirus Scanner** – installs the files that are required to perform on-demand virus scans. This feature is installed by default.

  The Command AntiVirus Scanner contains the following subfeatures:

  - **Shell Extension** – adds the Command AntiVirus Scan option to the shell shortcut menu. This subfeature is installed by default.

  - **Help Files** – installs the Command AntiVirus online help files. By default, this subfeature is installed the first time it is accessed.

- **Dynamic Virus Protection** – installs the files that are required to perform on-access virus scans. This feature is installed by default.

- **Optional Files** – installs the files that are required for additional Command AntiVirus features. This feature is installed by default.

  Optional Files contains the following subfeatures:

  - **Scheduled Update** – installs the files that are required to perform a scheduled update. This subfeature is installed by default.

  - **Communication System** – installs the files that are required by CSS Central to remotely administer computers that are running Command AntiVirus. This subfeature is installed by default.

  - **NetWare Reporting** – installs the files that are required for a workstation to communicate with a server that is running Command AntiVirus for NetWare. This subfeature is **not** installed by default.

NOTE: For **NetWare Reporting** to work, the Novell® NetWare® client **must** be installed.

  - **Scheduled Scan** – installs the files that are required to perform scheduled virus scans. This subfeature is installed by default.

- **Product Documentation** – installs the README.TXT and the Command AntiVirus Multi-Platform Quick Start Guide. This feature is installed by default.

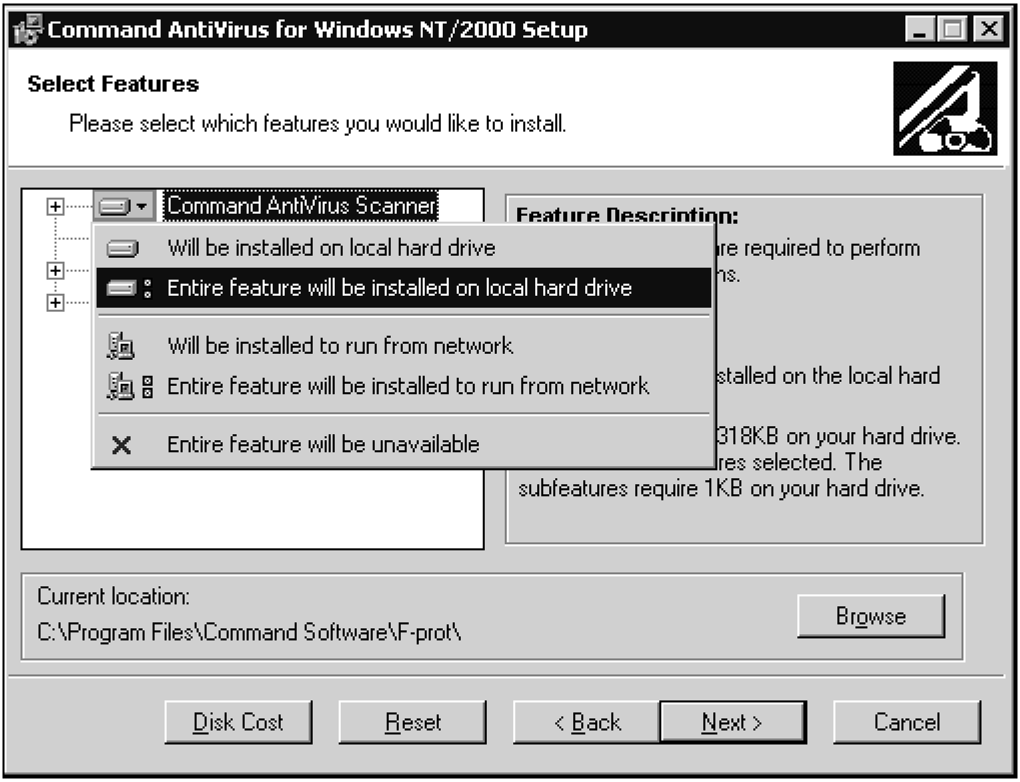
  Product Documentation contains the following subfeatures:

  - **Readme File** – installs the README.TXT file that contains the latest information on product enhancements, fixes and special instructions. This subfeature is installed by default.

  - **Quick Start** – installs the Command AntiVirus Multi-Platform Quick Start Guide. This subfeature is installed by default.

    The guide, which is located in the file called MQCKST.PDF, provides a brief overview of our products and basic start-up instructions. It can be viewed with Adobe® Acrobat® Reader.

To the left of each feature and subfeature is an icon that represents the present installation state. To view the explanation of each icon or to select a different installation state, click the down arrow to the right of the icon. The system displays a drop-down menu:



Command AntiVirus for Windows NT/2000 Setup

Select Features

Please select which features you would like to install.

Feature Descriptio

re required to perform
ns.

stalled on the local hard

318KB on your hard drive.
res selected. The
subfeatures require 1KB on your hard drive.

Current location:
C:\Program Files\Command Software\F-prot\

Command AntiVirus Scanner
Will be installed on local hard drive
Entire feature will be installed on local hard drive
Will be installed to run from network
Entire feature will be installed to run from network
Entire feature will be unavailable
Browse
Disk Cost
Reset
< Back
Next >
Cancel

Drop-Down Menu

NOTE: When the installation state of a subfeature is different from the state of the feature, the icon of the feature has a gray background.

Depending on the feature or subfeature that you select, the drop-down menu contains all or some of the following items:

Will be installed on local hard drive – installs the selected feature or subfeature on the local hard drive. If you select a subfeature, this option also installs the parent feature. For example, if you select to install the online **Help Files**, the **Command AntiVirus Scanner** is also installed.

Entire feature will be installed on local hard drive – installs the selected feature and all of its subfeatures on the local hard drive. For example, if you select the **Command AntiVirus Scanner**, the **Help Files** and the **Shell Extension** are also installed.

If you select a subfeature, this option installs the parent feature and the selected subfeature. For example, if you select to install **NetWare Reporting**, **Optional Files** is also installed.

Will be installed to run from network – installs the selected feature or subfeature on a network drive.

If you select a subfeature, this option also installs the parent feature. For example, if you select to install the online **Help Files**, the **Command AntiVirus Scanner** is also installed.

Entire feature will be installed to run from network – installs the selected feature and all of its subfeatures on a network drive.

If you select a subfeature, this option also installs the parent feature. For example, if you select to install **NetWare Reporting**, **Optional Files** is also installed.

Feature will be installed when required – installs the selected feature the first time it is accessed. For example, if you select this option for the online **Help Files, Help** is installed only the first time it is used.

NOTE: You **must** have Windows Desktop Update installed to be able to use the **Feature will be installed when required** installation state. Active Desktop does not have to be enabled.

Entire feature will be unavailable – does **not** install the selected feature or any of its subfeatures.

To change the installation state for a selected feature or subfeature, click the appropriate icon. The program returns to the **Select Features** dialog box which now shows the installation state icon that you selected.

Under **Current location**, you can change where the files are installed. The default is: `C:\Program Files\Command Software\F-prot\`. To select a different folder, use the **Browse** button.

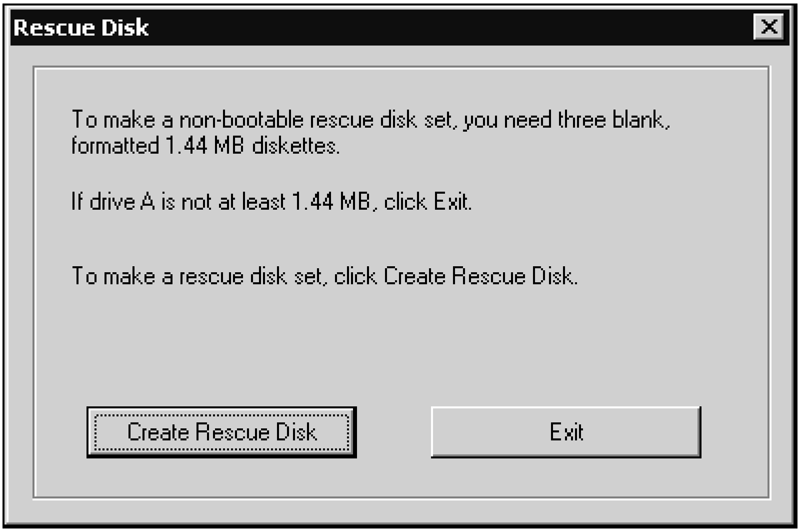
NOTE: You can change only the location of files that are unique to Command AntiVirus. Files that are shared among other Command AntiVirus products such as CSS Central are automatically stored in the system's **Common Files** folder.

NOTE: To reset the features and subfeatures to the default selections, click **Reset**. To view details of the amount of disk space that a feature or subfeature requires on the hard drive, click **Disk Cost**.

12. Click **Next** to begin the installation. The system displays the **Updating System** dialog box. Please wait while the program copies the Command AntiVirus files to your system.

NOTE: You can click **Cancel**, **Exit Setup** and then **OK** to cancel the installation and exit the setup program.

When the copying is complete, the system displays the **Rescue Disk** dialog box:



Rescue Disk

To make a non-bootable rescue disk set, you need three blank, formatted 1.44 MB diskettes.

If drive A is not at least 1.44 MB, click Exit.

To make a rescue disk set, click Create Rescue Disk.

Rescue Disk Dialog Box

To create a rescue disk set, you **must** be a member of the local Administrators group.

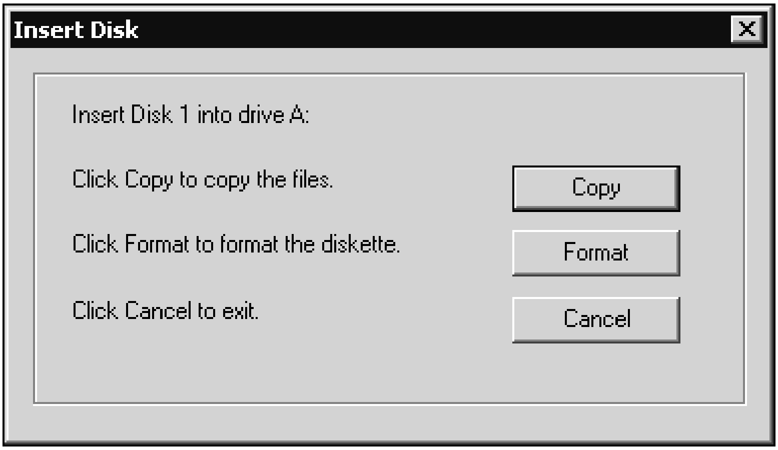
NOTE: To create a rescue disk set, you will need three blank, formatted 1.44 MB diskettes labeled **CSAV Rescue Disk 1 for (User's Computer ID)**, **CSAV Rescue Disk 2 for (User's Computer ID)**, and **CSAV Rescue Disk 3 for (User's Computer ID)**.

For NTFS systems, unless you can access an NTFS drive from within DOS, for example, by using third-party software, you will **not** be able to use the rescue disk set to scan files on an NTFS drive.

You can use **Rescue Disk 1** on NTFS systems at any time to repair damaged or infected boot sector information.

NOTE: If drive A is not at least 1.44 MB or you do not want to create a rescue disk set, click **Exit**.

13. To make a non-bootable rescue disk set, click **Create Rescue Disk**. The system displays the **Insert Disk** dialog box:



Insert Disk

Insert Disk 1 into drive A:

Click Copy to copy the files.

Click Format to format the diskette.

Click Cancel to exit.

Insert Disk Dialog Box

14. Insert **Disk 1** into drive A and click **Copy**. The system returns to the **Rescue Disk** dialog box which displays the files being copied.

    To format a diskette, click **Format**. Then, continue with the formatting process. When the formatting process is complete, click **Close** to return to the **Insert Disk** dialog box.

15. When the copying is complete, the system displays a dialog box informing you that the rescue disk was created successfully. Click **OK** to continue. The system displays the **Insert Disk** dialog box.

16. Remove **Disk 1** from drive A, and set the write-protect tab to prevent any modifications.

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

17. Insert **Disk 2** into drive A and click **Copy**. The system returns to the **Rescue Disk** dialog box which displays the files being copied.
18. When the copying is complete, the system displays a dialog box informing you that the rescue disk was created successfully. Click **OK** to continue. The system returns to the **Rescue Disk** dialog box.
19. Remove **Disk 2** from drive A, and set the write-protect tab to prevent any modifications.
20. Insert **Disk 3** into drive A and click **Copy**. The system returns to the **Rescue Disk** dialog box which displays the files being copied.
21. When the copying is complete, the system displays a dialog box informing you that the rescue disk was created successfully. Click **OK** to continue. The system returns to the **Rescue Disk** dialog box.
22. Remove **Disk 3** from drive A, and set the write-protect tab to prevent any modifications.
23. Click **Exit**. The system displays a dialog box informing you that Command AntiVirus for Windows NT/2000 has been successfully installed.
24. Click **Finish** to exit.

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 Shortcut

You may want to create a shortcut on the desktop for easy access to Command AntiVirus. There are many ways to create shortcuts. The following is one example. This example is based on using the default installation location.

1. Using the right mouse button (right-click), click the desktop.
2. Select **New**.
3. Click **Shortcut**.
4. Click **Browse** to locate the **Program Files** folder.
5. Double-click **Program Files**.
6. Double-click **Command Software**.
7. Double-click **F-PROT**.
8. Select **F-PROT32.EXE** and click **OK**.
9. Click **Next** to continue.
10. Type **Command AntiVirus** in the **Select a name for the shortcut** text box.
11. Click **Finish**.

CREATING A RESCUE DISK SET

To create a rescue disk set, you **must** be a member of the local Administrators group.

If you did not choose to make a Command AntiVirus rescue disk during installation, you can create one from the **Rescue Disks** menu on the menu bar.

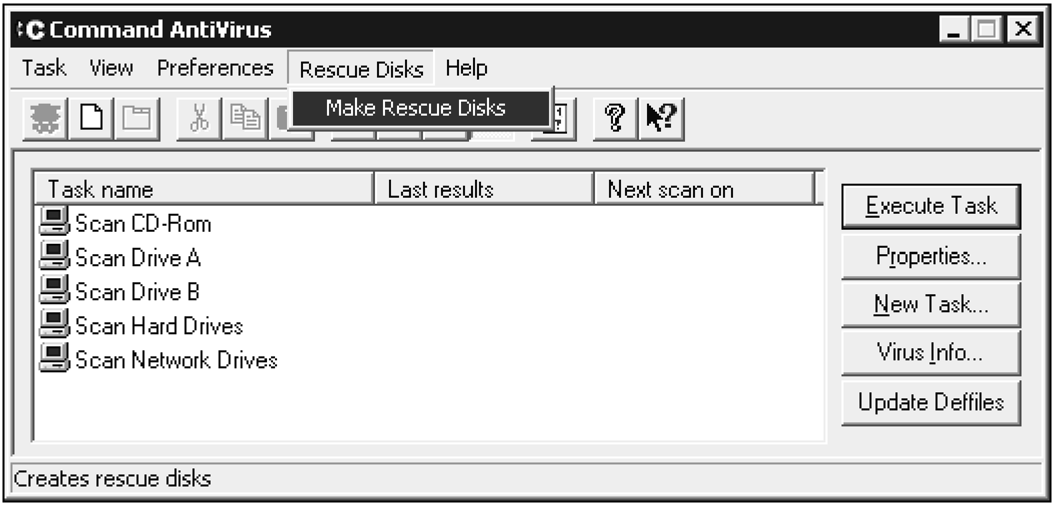
NOTE: To create a rescue disk set, you will need three blank, formatted 1.44MB diskettes labeled **CSAV Rescue Disk 1 for (User's Computer ID)**, **CSAV Rescue Disk 2 for (User's Computer ID)**, and **CSAV Rescue Disk 3 for (User's Computer ID)**. Also, make sure that the diskettes and your system are **virus-free**.

For NTFS systems, unless you can access an NTFS drive from within DOS, for example, by using third-party software, you will **not** be able to use the rescue disk set to scan files on an NTFS drive.

You can use **Rescue Disk 1** on NTFS systems at any time to repair damaged or infected boot sector information.

To create a rescue disk set, follow these steps:

1. On the menu bar, click **Rescue Disks**. The system displays the drop-down menu:

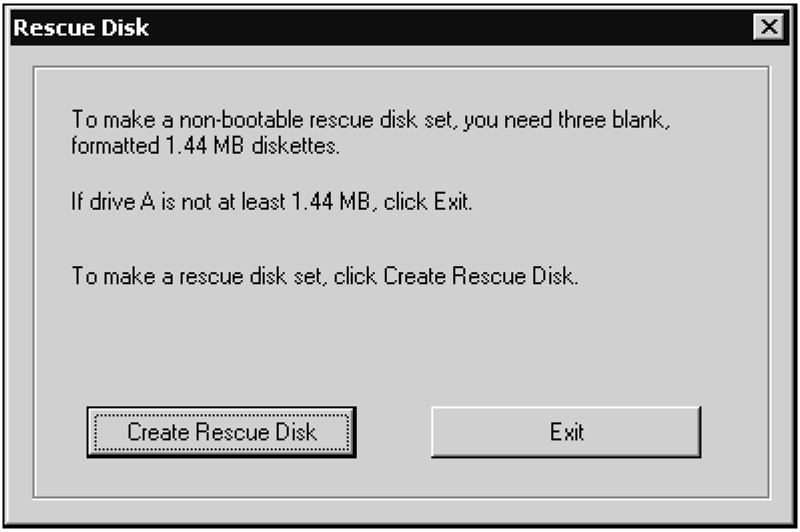


Task name	Last results	Next scan on
Scan CD-Rom		
Scan Drive A		
Scan Drive B		
Scan Hard Drives		
Scan Network Drives		

Creates rescue disks

Make Rescue Disks

2. Click **Make Rescue Disks**. The system displays the **Rescue Disk** dialog box:



Rescue Disk

To make a non-bootable rescue disk set, you need three blank, formatted 1.44 MB diskettes.

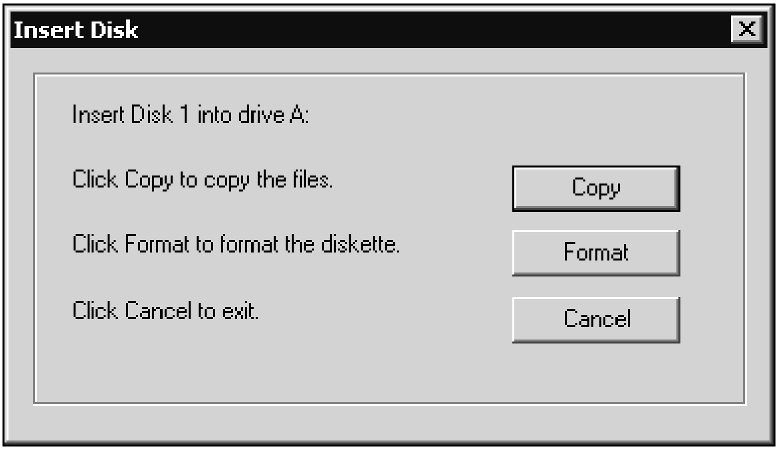
If drive A is not at least 1.44 MB, click Exit.

To make a rescue disk set, click Create Rescue Disk.

Rescue Disk Dialog Box

NOTE: If drive A is not at least 1.44 MB, or you do not want to create a rescue disk set, click **Exit**.

3. To make a non-bootable rescue disk set, click **Create Rescue Disk**. The system displays the **Insert Disk** dialog box:



Insert Disk 1 into drive A:

Click Copy to copy the files.

Click Format to format the diskette.

Click Cancel to exit.

Insert Disk Dialog Box

4. Insert **Disk 1** into drive A and click **Copy**. The system returns to the **Rescue Disk** dialog box which displays the files being copied.

   To format a diskette, click **Format**. Then, continue with the formatting process. When the formatting process is complete, click **Close** to return to the **Insert Disk** dialog box.

5. When the copying is complete, the system displays a dialog box informing you that the rescue disk was created successfully. Click **OK** to continue. The system displays the **Insert Disk** dialog box

6. Remove **Disk 1** from drive A, and set the write-protect tab to prevent any modifications.

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

7. Insert **Disk 2** into drive A and click **Copy**. The system returns to the **Rescue Disk** dialog box which displays the files being copied.

8. When the copying is complete, the system displays a dialog box informing you that the rescue disk was created successfully. Click **OK** to continue. The system returns to the **Rescue Disk** dialog box.
9. Remove **Disk 2** from drive A, and set the write-protect tab to prevent any modifications.
10. Insert **Disk 3** into drive A and click **Copy**. The system returns to the **Rescue Disk** dialog box which displays the files being copied.
11. When the copying is complete, the system displays a dialog box informing you that the rescue disk was created successfully. Click **OK** to continue. The system returns to the **Rescue Disk** dialog box.
12. Remove **Disk 3** from drive A, and set the write-protect tab to prevent any modifications.
13. Click **Exit**. The system returns to the **CSAV Main** dialog box.

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 on only the computer that was used to create the file.

TESTING THE RESCUE DISK SET

To test 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
```

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.

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

USING THE RESCUE DISK SET

Dealing with some viruses may require the use of your rescue disk set. The rescue disk process involves two phases.

The first phase focuses on recovery by detecting and removing any executable, boot sector, and MBR-infecting viruses that inhibit or prevent system startup.

After successful recovery, the second phase focuses on scanning and disinfecting all remaining virus-infected files, for example, macro virus-infected files.

To assure a successful rescue, you **must** perform both phases.

To perform Phase One, 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
```

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.
11. Proceed to **Phase Two**.

To perform Phase Two, follow these steps:

1. Restart your computer as normal.
2. Use Command AntiVirus to perform a scan of your local hard drives. This scan detects and disinfects any remaining virus-infected files on your computer.

After completing the **Phase Two** scan, you can return to computing as normal.

INSTALLATION MAINTENANCE

After you have installed Command AntiVirus, you can add or remove features, reinstall Command AntiVirus, and remove Command AntiVirus through the installation program's **Application Maintenance** dialog box.

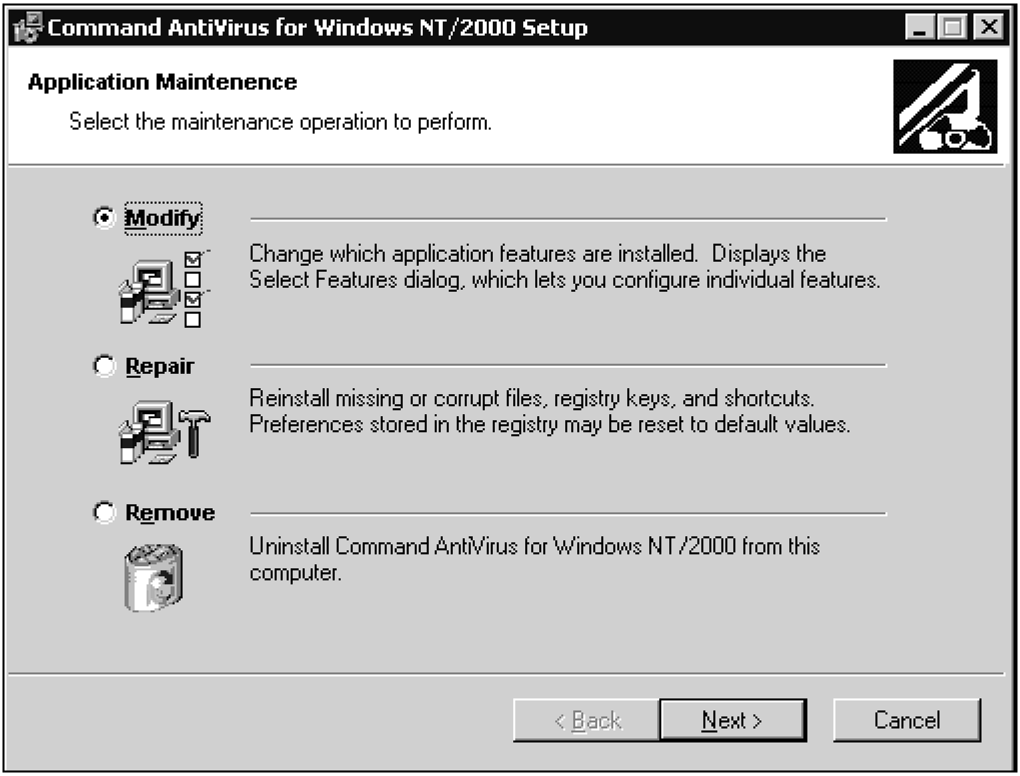
NOTE: You can also remove Command AntiVirus by clicking the **Remove** button in the Windows 2000 **Add/Remove Programs** dialog box.

To start the installation program, follow these steps:

1. Click the **Start** button on the Windows taskbar.
2. Select **Settings**.
3. Click **Control Panel**.

4. Click **Add/Remove Programs**. The system displays the **Add/Remove Programs** dialog box.

5. Select **Command AntiVirus for Windows NT/2000** from the list of currently installed programs, and click the **Change** button. The system displays the Command AntiVirus installation program's **Application Maintenance** dialog box:



Command AntiVirus for Windows NT/2000 Setup

Application Maintenence

Select the maintenance operation to perform.

● Modify

Change which application features are installed. Displays the Select Features dialog, which lets you configure individual features.

○ Repair

Reinstall missing or corrupt files, registry keys, and shortcuts. Preferences stored in the registry may be reset to default values.

○ Remove

Uninstall Command AntiVirus for Windows NT/2000 from this computer.

Application Maintenance Dialog Box

This dialog box contains the following operations:

- **Modify** – allows you to add or remove features or subfeatures.
- **Repair** – allows you to reinstall missing or corrupt files, registry keys, and shortcuts.

NOTE: Preferences stored in the registry may be reset to default values.

- **Remove** – allows you to remove Command AntiVirus completely.

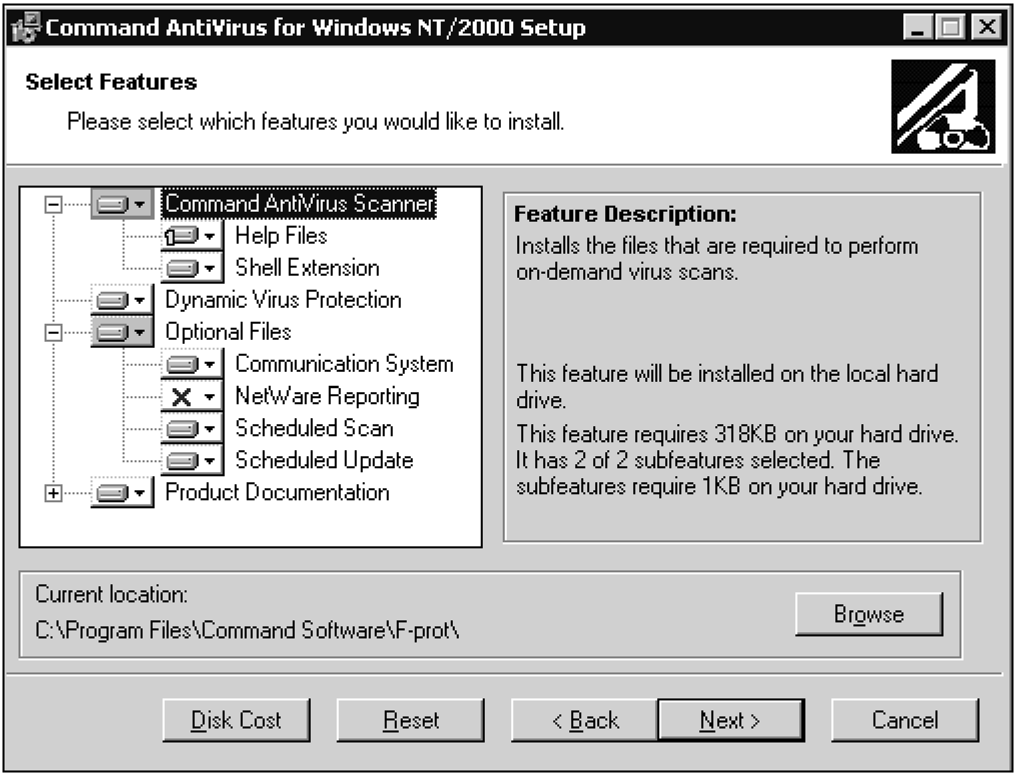
6. Go to the instructions for the operation that you want to perform, for example, **Adding or Removing Features**.

ADDING OR REMOVING FEATURES

After you have installed Command AntiVirus, you can add or remove features through the installation program's **Application Maintenance** dialog box. Refer to **Steps 1** through **6** in the **Installation Maintenance** section located previously in this chapter.

To add or remove features, follow these steps:

1. In the Command AntiVirus installation program's **Application Maintenance** dialog box, select **Modify**, and click **Next**. The system displays the **Select Features** dialog box:



Select Features

Please select which features you would like to install.

- Command AntiVirus Scanner
  - Help Files
  - Shell Extension
- Dynamic Virus Protection
- Optional Files
  - Communication System
  - NetWare Reporting
  - Scheduled Scan
  - Scheduled Update
- Product Documentation

Feature Description:

Installs the files that are required to perform on-demand virus scans.

This feature will be installed on the local hard drive.

This feature requires 318KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 1KB on your hard drive.

Current location:

C:\Program Files\Command Software\F-prot\

Select Features Dialog Box

2. Select or cancel the selection of the features or subfeatures that you want to add or remove. Click the plus sign to (+) to display the subfeatures.

   To select a different installation state, click the down arrow ▾ to the right of the icon. For more information, refer to **Custom Installation** located previously in this chapter.

NOTE: To reset the features and subfeatures to the selections of the previous installation, click **Reset.** To view details of the amount of disk space that a feature or subfeature requires on the hard drive, click **Disk Cost**.

3. Click **Next** to begin. The system displays the **Updating System** dialog box. Please wait while the program updates your system.

NOTE: You can click **Cancel**, **Exit Setup** and then **OK** to cancel the install and exit the setup program.

4. When the updating is complete, the system displays a dialog box informing you that Command AntiVirus for NT/2000 has been successfully installed. Click **Finish** to exit.

REINSTALLING COMMAND ANTIVIRUS

You can repair the Command AntiVirus installation through the installation program’s **Application Maintenance** dialog box. Refer to **Steps 1** through **6** in the **Installation Maintenance** section located previously in this chapter.

This option allows you to reinstall missing or corrupt files, registry keys, and shortcuts.

NOTE: Preferences stored in the registry may be reset to default values.

To reinstall Command AntiVirus, follow these steps:

1. In the Command AntiVirus installation program’s **Application Maintenance** dialog box, select **Repair**, and click **Next**. The system displays the **Ready to Repair the Application** dialog box.

NOTE: You can click **Back** to make a new selection, or you can click **Cancel**, **Exit Setup** and then **OK** to cancel the reinstallation and exit the setup program.

2. Click **Next** to begin the installation. The system displays the **Updating System** dialog box. Please wait while the program copies the Command AntiVirus files to your system.

NOTE: You can click **Cancel**, **Exit Setup** and then **OK** to cancel the reinstallation and exit the setup program.

3. When the copying is complete, the system displays a dialog box informing you that Command AntiVirus for NT/2000 has been successfully installed. Click **Finish** to exit.

REMOVING COMMAND ANTIVIRUS

You can completely remove an installed version of Command AntiVirus through the installation program's **Application Maintenance** dialog box. Refer to **Steps 1** through **6** in the **Installation Maintenance** section located previously in this chapter.

To remove Command AntiVirus completely, follow these steps:

1. In the Command AntiVirus installation program's **Application Maintenance** dialog box, select **Remove**, and click **Next**. The system displays the **Uninstall** dialog box.
2. Click **Next** to remove Command AntiVirus. The system displays the **Updating System** dialog box. Please wait while the program removes the Command AntiVirus files from your system.

NOTE: You can click **Cancel**, **Exit Setup** and then **OK** to cancel the uninstall and exit the setup program.

3. When the removal is complete, the system displays a dialog box informing you that Command AntiVirus for NT/2000 has been successfully uninstalled. Click **Finish** to exit.

USING COMMAND ANTIVIRUS

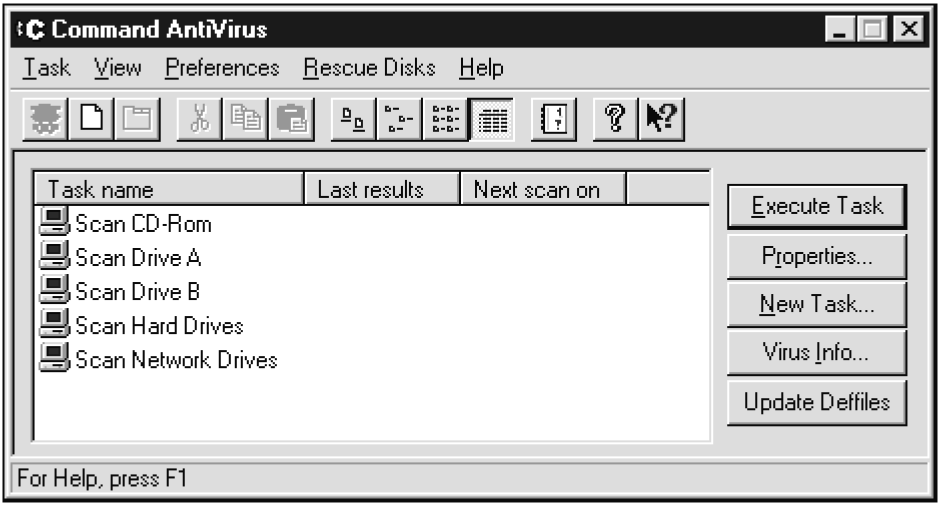
Command AntiVirus for Windows NT®/2000 (CSAV) provides an effective and easy way to scan for viruses. It allows administrators to customize the default virus scanning tasks and to create new scanning tasks that can be modified only by someone who has administrative rights. Users without administrative rights can create their own scan tasks to suit their particular needs.

In addition, Command AntiVirus for Windows NT/2000 includes the CSS AV Scheduler service that runs scheduled scans and inactivity scans in the background. With this feature, the user’s work flow is not interrupted while the product’s anti-virus protection operates invisibly behind the scenes.

The following sections describe the many features that allow you to modify Command AntiVirus to your specifications.

THE CSAV MAIN DIALOG BOX

Command AntiVirus uses a graphical user interface (GUI) that allows you to customize, start, and schedule virus scans quickly and easily. The main screen of the GUI is called the **Command AntiVirus Main** dialog box:



Command AntiVirus Main Dialog Box

From the **Command AntiVirus Main** dialog box, you can perform numerous scan task operations. For example, you can set the folder to which detected viruses are quarantined. You can also create, delete, modify, select, start, and enable/disable virus scans.

Configuring individual scan tasks is possible through the easy-to-use options found in the menu bar, toolbar, or command buttons. You can use the **Task List** to access all major configuration features for an individual scan task. For example, to change a scan task’s properties, select the scan task name in the **Task List** and click the **Properties** button.

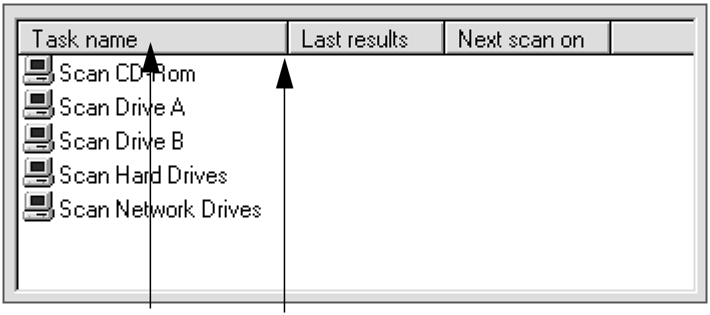
The menu bar contains **Task**, **View**, **Preferences**, **Rescue Disk**, and **Help** menus that you can use to configure Command AntiVirus, create a rescue disk set, or find help on how to use the product’s features.

TASK WINDOW

The main feature in the **Command AntiVirus Main** dialog box is the **Task Window**. This window contains a **Task List** with **Task names** identifying the available scan tasks. The **Last Results** column shows the results of the last scan. The **Next Scan On** column shows the time of the next scheduled on-demand scan.

ABOUT THE TASK LIST

From the **Task List**, you can create, configure, and start scan tasks. For example, you can set the properties of a scan task, set up a scheduled scan, or create a new scan task.



Task name	Last results	Next scan on
Scan CD-Rom		
Scan Drive A		
Scan Drive B		
Scan Hard Drives		
Scan Network Drives		

Task List in Details View

Command AntiVirus comes with several preconfigured tasks that are available upon installation. These include the most commonly needed tasks:

- scan cd-rom drives
- scan drive a
- scan drive b
- scan hard drives
- scan network drives

To start one of the existing scan tasks from the **Task List**, just double-click the task name.

Types of Scan Tasks

Two types of scans can be created:

- **Administrator Tasks –** Scans created by someone with administrator rights. You can identify an **Administrator Task** by the computer icon to the left of the scan task name.
- **User Tasks –** Scans created by a user without administrator rights. You can identify a **User Task** by the profile icon to the left of the scan task name.

The preconfigured tasks that come with Command AntiVirus are **Administrator Tasks**.

NOTE: A user with administrator rights can create either type of task.

This difference between tasks allows administrators to create system-wide scanning tasks that cannot be modified or renamed by users who do not have administrator rights.

NOTE: If multiple users create customized **User Tasks**, those tasks are visible only to the user who is currently logged in. This is because they are stored in the user's profile directory.

Sizing the Columns

If you select **Details** from the **View** menu, the **Task Window** displays column headers. You can resize the headers by using your mouse pointer to drag the header's left or right split bar.

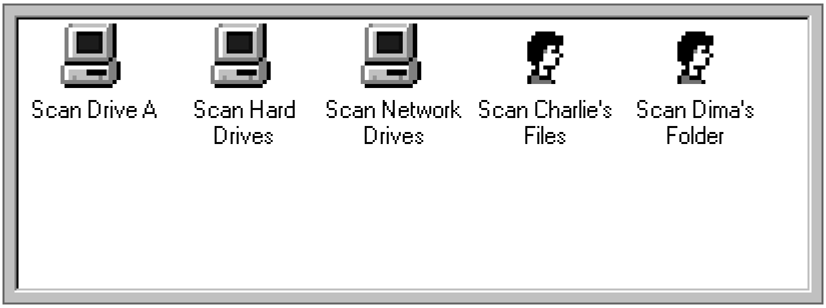
Sorting the Order of Scan Tasks

You can sort scan tasks in the **Task List** by clicking the column headers. For example, clicking the **Last results** header alphabetically sorts scan tasks that detected a virus. Clicking the **Next scan on** header sorts scan tasks based on the next scheduled scans.

Changing the Icon Size of Scan Tasks

You can change the size of scan task icons by selecting **Large Icons** or **Small Icons** from the **View** menu. You can also click the **Large Icons** button or the **Small Icons** button on the toolbar.

The **Large Icons** view displays the scan task name below each icon. The **Small Icons** view displays the scan task name to the right of each icon. These views do **not** show the column headers, the results of the last scan conducted, or the next scheduled scan time.



Large Icons View

List or Details View of Scan Tasks

You can also view the **Task List** with or without details about each scan task.

Select **List** from the **View** menu to display a single column of small icons with the scan task name located to the right of each icon.

Select **Details** from the **View** menu to display the **Task List** with three column headers: **Task name**, **Last results**, and **Next scan on**.

The **Task name** column contains small icons with the scan task name located to the right of each icon. The **Last results** column contains the results of the last scan if a virus was found. The **Next scan on** column contains the time of the next scheduled scan. This is the only viewing option that displays column headers.

You can also click the **List** button or the **Details** button on the toolbar to switch between listing tasks or showing tasks with details.

Changing Task Names

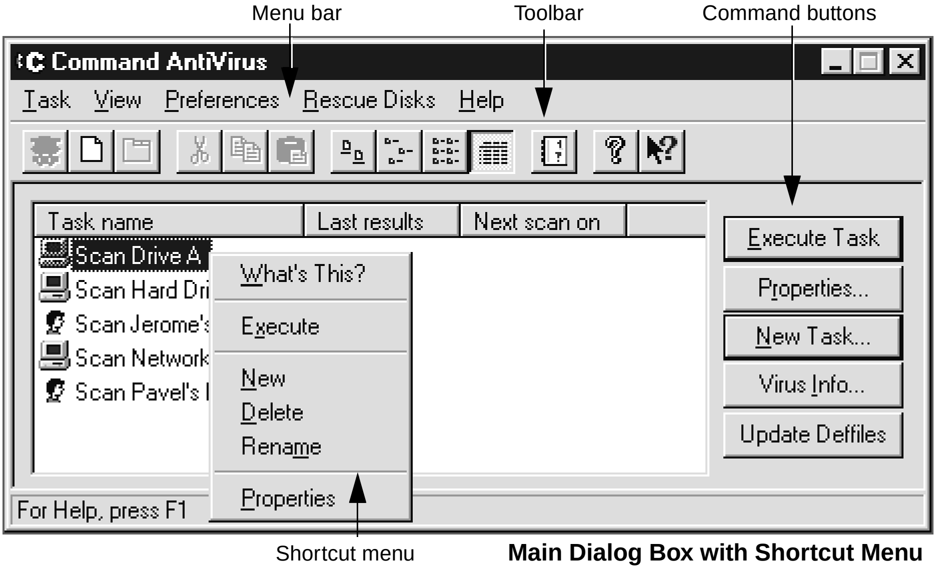
If you have administrator rights, you can rename any of the scan tasks by selecting the scan task and clicking once. You can also right-click the scan task and select **Rename** from the drop-down menu. Both of these actions open a text box around the existing name so that you can modify the scan task name. If you make an error while you are typing, press the **Esc** key to go back to the original name. When you are finished typing the name, press **Enter**.

NOTE: Use **only** those characters that are legal for the operating system's long file name format. For example, a scan task name **cannot** contain a \ (backslash) character.

If you do **not** have administrator rights, you can change the name of **User Tasks**, but **not** the name of **Administrator Tasks**. For more information, refer to **Types of Scan Tasks** located previously in this chapter.

USING THE CSAV MAIN DIALOG BOX

From the **Command AntiVirus Main** dialog box, you can access the Command AntiVirus functions in several ways. For example, you can use the command buttons, the menu bar, keyboard shortcuts or the toolbar to start scans or modify their properties.



Main Dialog Box with Shortcut Menu

COMMAND BUTTONS

The command buttons allow you to perform various scan task operations. For example, you can create, modify or start a selected scan task. You can also access a list of known viruses that Command AntiVirus detects or update your virus definition files.

Execute Task Button

This button allows you to start an on-demand scan. Select the scan task that you want to start and click **Execute Task**. For more information on starting an on-demand scan, refer to **Executing a Scan** located later in this chapter.

Properties Button

This button allows you to configure the scan task. Select the scan task that you want to modify and click **Properties**. For more information on configuring a scan task, refer to **Configuring Scanning Properties** located later in this chapter.

New Task Button

This button allows you to create a new scan task. Just click the **New Task** button. For more information on creating new scan tasks, refer to **Creating New Tasks** located later in this chapter.

Virus Info Button

This button allows you to access a list of known viruses that Command AntiVirus detects. This list is updated each time you update your virus definition files. Just click **Virus Info**.

Update Deffiles Button

This button allows you to update the Command AntiVirus definition files on-demand.

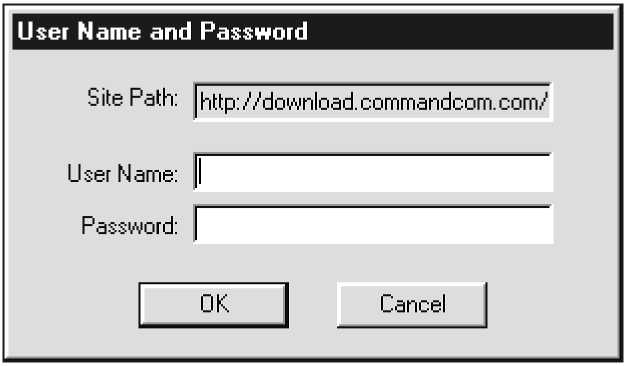
✓ **NOTE:** To use the **Update Deffiles** button, your computer **must** be able to be connected to the Internet.

By default, CSAV first tries to connect to the Command AntiVirus web site. If this attempt is unsuccessful, it then tries to connect to the Command AntiVirus FTP site.

To update the deffiles, follow these steps:

1. Click the **Update Deffiles** button. The system displays the **User Name and Password** dialog box.

NOTE: After you enter a **<u>valid</u>** user name and password for a specific **Site Path**, this dialog box does **<u>not</u>** display again as long as your user name and password for that site remain valid.



User Name and Password

Site Path: http://download.commandcom.com/

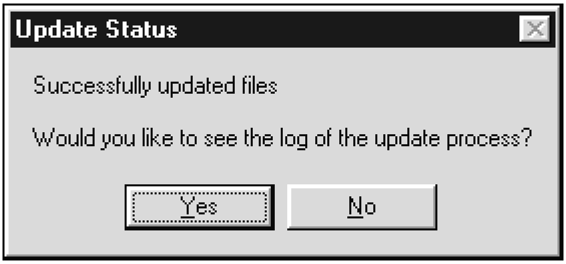
User Name:

Password:

User Name-Password Dialog Box

2. In the **User Name** text box, type your user name.
3. In the **Password** text box, type your password.
4. Click **OK**. CSAV attempts to make the connection and downloads the definition files if new files are available.

   When the process is complete, the system displays the **Update Status** dialog box:



Update Status

Successfully updated files

Would you like to see the log of the update process?

Update Status Dialog Box

This dialog box displays the status of the download, for example:

```
Successfully updated files
```

It also gives you the option to view the details of the status in the log file.

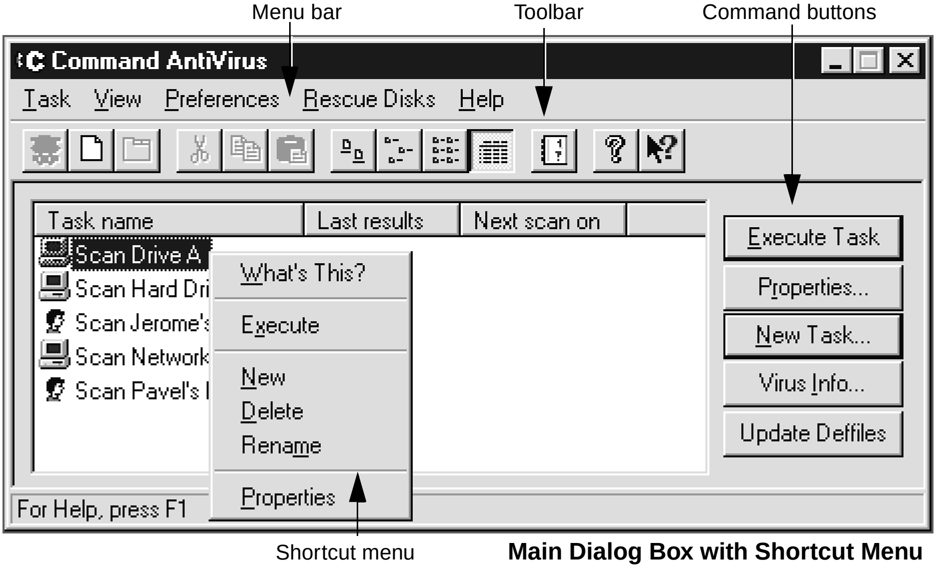
5. Click **No** to continue.

System administrators can set which update sites the **Update Deffiles** button uses through the **Preferences**/**Advanced**/**Update Deffiles Now** dialog box. For more information, see **Definition Files Update Button** in the ***Network Administration*** chapter.

SHORTCUT MENU

This menu allows you to start, create, delete, rename, or modify the properties of a scan task.

You can quickly access a shortcut menu by selecting a scan task and right-clicking it.



Main Dialog Box with Shortcut Menu

MENU BAR

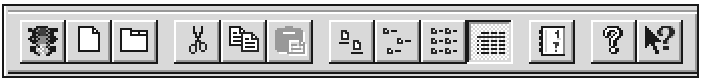
From the menu bar, you can access the **Task**, **View**, **Preferences**, **Rescue Disks**, and **Help** menus with the mouse or keyboard. Just click one of the menu titles and select a menu item. Or, use the keyboard by pressing the **ALT** key plus the underlined letter for the menu title or item.

These menus contain items that allow you to perform any of the operations available for starting, creating, deleting, or modifying scan tasks. You can also change the way you view the tasks, customize Command AntiVirus, create a rescue disk, or view topics that contain helpful information.

Detailed information on using these menus is provided later in this chapter.

TOOLBAR BUTTONS

The toolbar provides quick access to functions that can also be accessed from other menus. For example, you can start, create, modify, and delete scan tasks. You can also get help and change the way your screen looks. Just click the appropriate button.



NOTE: To see a ToolTip that identifies the function of a particular button, move the mouse pointer over any toolbar button.

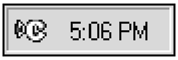
Help

This button adds a question mark to the mouse pointer. When you point and click an object, the system displays a help screen containing information that is relevant to that object.

OTHER WAYS TO ACCESS COMMAND ANTIVIRUS

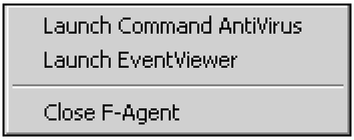
You can open the **Command AntiVirus Main** dialog box in several ways:

- From the **Start** menu.
- By double-clicking the yellow **C** icon (F-Agent icon) located in the system tray at the bottom right of your screen:



F-Agent Icon

- By right-clicking the yellow **C** icon in the system tray and then clicking **Launch Command AntiVirus** from the **F-Agent Shortcut Menu:**



F-Agent Shortcut Menu

The **F-Agent Shortcut** menu also allows you to open **Event Viewer** or close F-Agent.

NOTE: If you close F-Agent, the yellow **C** icon is no longer visible and inactivity scans do not work. Although you cannot see the little clock running, scheduled scans and DVP continue to function.

To restart F-Agent follow these steps:

1. On the Windows task bar, click **Start**. The system displays the **Start** menu.
2. Click **Run**. The system displays the **Run** dialog box.
3. In the **Open** text box, type **f-agent**.

NOTE: If you have not logged in since first installing Command AntiVirus, you will need to use the **Browse** button to search for the complete path.

4. Click **OK**.

QUICK SCANNING

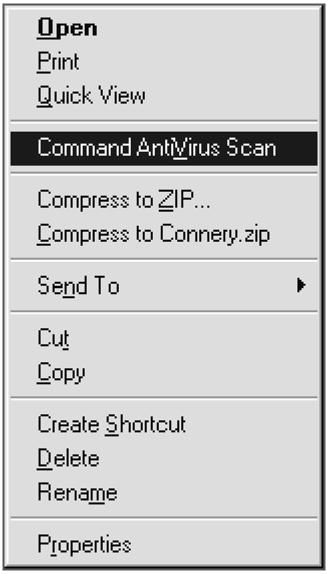
You can perform a quick scan of a specific file or folder by using the right-click shortcut feature or the drag and drop feature.

Using the Shortcut Menu

You can activate a shortcut menu that allows you to perform fast and efficient virus scans of selected folders or files. The files or folders to be scanned can be located in Windows Explorer, on the desktop, or within program groups.

To perform a scan from the shortcut menu, follow these steps:

1. Select one or more file names or folders that you want to scan.
2. With the mouse pointer on the selected items, right-click. The operating system displays a shortcut menu containing the **Command AntiVirus Scan** option:



Shortcut Menu Scan

3. Click **Command AntiVirus Scan**. The scan begins immediately

When the scan is complete, the system displays a report window.

NOTE: The shortcut or right-click scanning properties are based on the Command AntiVirus default scanning properties. For example, if a virus is found, you receive only a notification. You must then scan the file with a task that allows disinfection or whatever action you use for viruses.

USING COMMAND ANTIVIRUS

Administrators can customize the shortcut menu scan as follows:

1. Click the **New Task** button. The system displays the **Create New Task** dialog box.
2. In the text box, type **R-Mouse**. It is necessary to use only this task name. The name is not case sensitive, but you cannot include spaces.
3. Click **OK**. The system displays the **Properties** dialog box.

NOTE: Anything entered under **Path/Drives to scan** is ignored, and the selected file(s) or folders are scanned instead.

4. In **File types to scan,** select the appropriate options. For more information, refer to **Configuring Scanning Properties** located later in this chapter.
5. In **Action to take**, select **one** of the available options.
6. Click **OK**. The system returns to the **Command AntiVirus Main** dialog box.
7. Exit Command AntiVirus.

Now, when you want to perform a scan from the shortcut menu, the scan will be based on your customized settings.

Using Drag-and-Drop

Another way to scan files quickly is to use the drag-and-drop feature in Command AntiVirus.

To perform a scan using drag-and-drop, follow these steps:

1. Open the **Command AntiVirus Main** dialog box on your desktop.

2. From Windows Explorer or from the desktop, drag the files or folders anywhere over the **Task Window**.
3. Release the mouse button. The scan starts immediately.

When the scan is complete, the system displays a report window.

NOTE: The drag-and-drop properties are based on the Command AntiVirus default scanning properties. For example, if a virus is found, you receive only a notification. You must then scan the file with a task that allows disinfection or whatever action you use for viruses.

Administrators can customize the drag and drop scan as follows:

1. Click the **New Task** button. The system displays the **Create New Task** dialog box.
2. In the text box, type **DragDrop**. It is necessary to use only this task name. The name is not case sensitive, but you cannot include spaces.
3. Click **OK**. The system displays the **Properties** dialog box.

NOTE: Anything entered under **Path/Drives to scan** is ignored, and the selected file(s) or folders are scanned instead.

4. In **File types to scan,** select the appropriate options. For more information, refer to **Configuring Scanning Properties** located later in this chapter.
5. In **Action to take**, select <u>**one**</u> of the available options.
6. Click **OK**. The system returns to the **Command AntiVirus Main** dialog box.
7. Exit Command AntiVirus.

Now, when you want to perform a scan using drag and drop, the scan will be based on your customized settings.

SCANNING FROM THE COMMAND LINE

There are times when it is useful to run a scan directly from the command line. For example, command-line entries allow an administrator who is logging in remotely to start a scan immediately.

Command AntiVirus provides two programs that you can use to run a scan from the command line. They are **CSAVNTC.EXE** and **CSS-AVS.EXE** (CSS AV Scheduler).

CSAVNTC.EXE is an operating system-specific command-line scanner that is included with Command AntiVirus for Windows NT/2000. It provides the same state-of-the-art protection as our graphical user interface and on-access scanners. For more information, refer to the **GUIDE.TXT** file that is located in the Command Software\F-PROT folder.

You can also use **CSS-AVS.EXE** to run scheduled and inactivity scans in the background or to run on-demand scans.

To use this feature, type **CSS-AVS.EXE**, and then add one or more of the available command-line parameters.

You can add command-line parameters in any order except for **/FILE**, **/PATH** and **/TASK**. These three parameters **must** be placed last on the command line and **must** be used only **one** at a time.

The following example starts a scan that checks memory, scans all logical hard drives, and disinfects any viruses that are detected.

```
CSS-AVS /MEM /HARD /DISINF
```

If viruses are detected, they are logged into the operating system’s **Event Viewer Application Log**.

TABLE 1: COMMAND LINE PARAMETERS FOR CSS AV SCHEDULER

Switch	Description
/DELETE	Deletes all infected files instead of listing them. This is **not** recommended as some viruses encrypt portions of the drive.
/DENY	Denies access to files containing a virus.
/DIR	Scans subdirectories.
/DISINF	Disinfects whenever possible. This option does delete some first-generation virus samples. A first-generation virus is the “starter” program that begins the infection process. It is very rare to encounter one. This option never deletes a file that can be disinfected.
/FILE=*filename*	Scans for file viruses. This switch **must** be last on the command line.
/FLOPPY	Scans floppy drives.
/HARD	Scans all the physical hard drives in the system.
/INSTALL	Installs the CSS AV Scheduler service into the Service Control Manager. *This must be run from the directory to which the service was installed (by default, Winnt/System32).
/MEM	Scans memory.
/MBR	Scans for MBR and boot sector viruses.
/NET	Scans network drives.
/PATH=*pathname*	Scans the specific path for viruses. This switch **must** be last on the command line.
/QUAR	Quarantines files containing a virus.
/RENAME	Renames infected files.
/REPORT	Sends the output to the specified file.

TABLE 1: COMMAND LINE PARAMETERS FOR CSS AV SCHEDULER

/TASK=*taskname*	Runs a specific scanning task. For example, “/TASK=c:\test.fpt /quar” runs the task called Test.fpt using the /QUAR switch. **Note:** You **must** include the .FPT extension in the task name. This switch **must** be last on the command line.
/UNINSTALL	Uninstalls the CSS AV Scheduler service from the Service Control Manager.

If you use the **/FILE=**, the **/PATH=**, or the **/TASK=** parameter, keep in mind that they **must** be used only one at a time, and they **must** be the last parameter entered on the command line.

LOCATING SCAN RESULTS IN EVENT VIEWER

If Command AntiVirus finds a virus during a scheduled scan or in real time through DVP, it logs the occurrence to the operating system’s **Event Viewer Application Log**.

There are several ways to access **Event Viewer** from within Command AntiVirus:

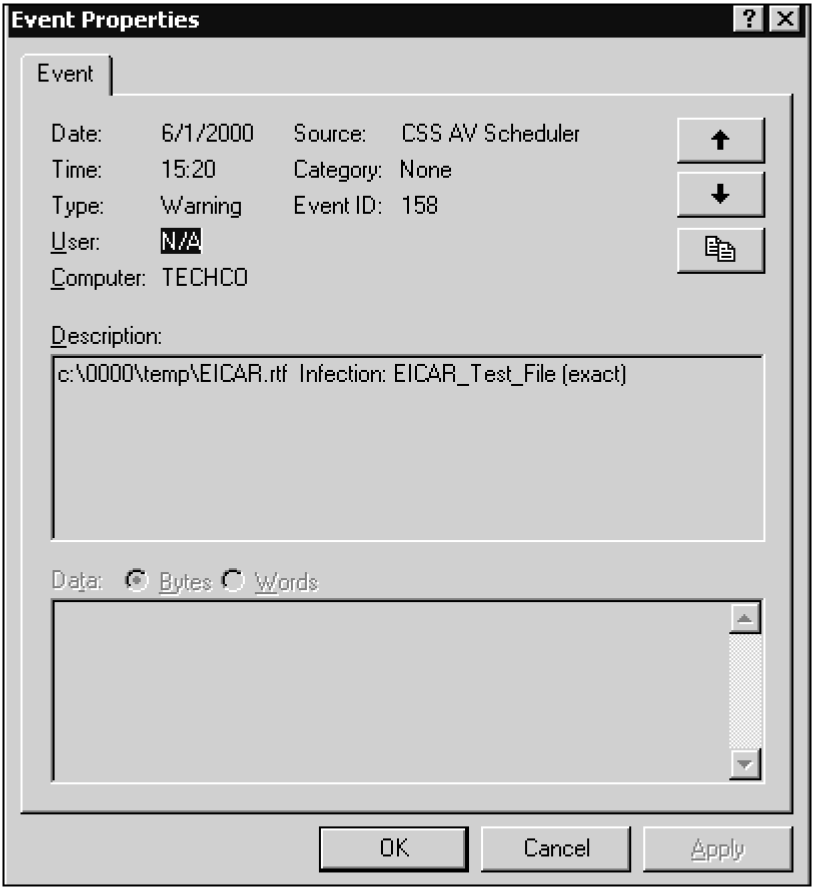
- Selecting **Event Viewer** from the **View** menu
- Clicking the **Event Viewer** button on the toolbar
- Right-clicking the yellow **C** icon at the bottom of the screen and selecting **Launch Event Viewer**

To locate the event in Windows 2000, follow these steps:

1. Open **Event Viewer**.
2. Select **Application Log**. For a virus reported by a scheduled scan, in the **Source** column of the log, look for **CSS AV Scheduler**.

   For a virus reported by DVP, in the **Source** column of the log, look for **CSS DVP**.

3. Double-click the event to view the **Event Properties** dialog box:



Date: 6/1/2000 Source: CSS AV Scheduler
Time: 15:20 Category: None
Type: Warning Event ID: 158
User: N/A
Computer: TECHCO

Description:
c:\0000\temp\EICAR.rtf Infection: EICAR_Test_File (exact)

Event Properties Dialog Box

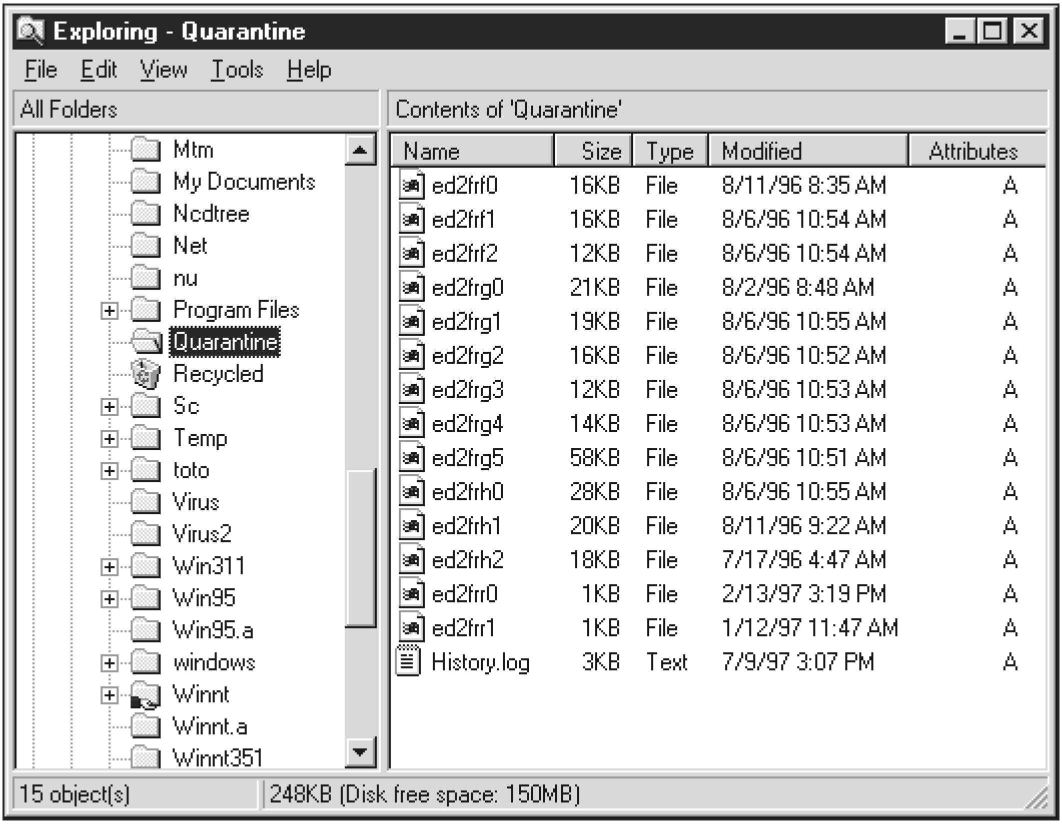
The **Event Properties** dialog box provides specific information on the viruses that were found during the scan. For more information on the Command AntiVirus messages in Event Viewer, refer to the ***Appendix***.

USING THE QUARANTINE FEATURE

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

The quarantine option is available for files that are scanned using specific tasks (scheduled and on-demand) and for files scanned in real time. To move infected files to the quarantine folder automatically, you **must** set the **Action to take** in the **Properties** and **Active Protection** dialog boxes to **Quarantine** or **Quarantine/ Query**. For more information, refer to **Configuring Scanning Properties** and **Active Protection** located later in this chapter.

When you select either of these options, by default, the **Quarantine** folder is created in the root directory of the system drive where Windows was installed. This folder is then used to hold infected files.



Name	Size	Type	Modified	Attributes
ed2frf0	16KB	File	8/11/96 8:35 AM	A
ed2frf1	16KB	File	8/6/96 10:54 AM	A
ed2frf2	12KB	File	8/6/96 10:54 AM	A
ed2frg0	21KB	File	8/2/96 8:48 AM	A
ed2frg1	19KB	File	8/6/96 10:55 AM	A
ed2frg2	16KB	File	8/6/96 10:52 AM	A
ed2frg3	12KB	File	8/6/96 10:53 AM	A
ed2frg4	14KB	File	8/6/96 10:53 AM	A
ed2frg5	58KB	File	8/6/96 10:51 AM	A
ed2frh0	28KB	File	8/6/96 10:55 AM	A
ed2frh1	20KB	File	8/11/96 9:22 AM	A
ed2frh2	18KB	File	7/17/96 4:47 AM	A
ed2frr0	1KB	File	2/13/97 3:19 PM	A
ed2frr1	1KB	File	1/12/97 11:47 AM	A
History.log	3KB	Text	7/9/97 3:07 PM	A

15 object(s) 248KB (Disk free space: 150MB)

Quarantine Folder

Administrators can change the location of the **Quarantine** folder by selecting **Advanced** from the **Preferences** menu and clicking the **Quarantine Path** tab. For more information refer to **Changing the Quarantine Folder** in the ***Network Administration*** chapter.

When a file is moved to the **Quarantine** folder, it is renamed. This is necessary as there can be files with the same names residing in different folders. If so, they would overwrite each other when they are moved to the **Quarantine** folder.

The new name that is created is alpha-numeric, using up to 8 characters.

For viruses that are detected through scheduled and on-demand scans, there is no extension.

For viruses that are detected in real time through Dynamic Virus Protection (DVP), a **.QUARANTINED** extension is added to the new file name.

If you use the quarantine feature, there are some important considerations that you need to be aware of:

- If the quarantine folder does not exist, Command AntiVirus creates it in the root directory. If a quarantine folder cannot be created or if there is an error in moving the infected file (for example, if the hard disk is full), the **Action on infection** for real-time scanning becomes **Report only**.
- If the **Action to take** for a scheduled or on-demand scan is **Quarantine** or **Quarantine/Query**, you **cannot** select **Scan quarantined files** located in the Command AntiVirus **Properties** dialog box.
- There are some items that you **cannot** quarantine. They are the MBR (Master Boot Record) and the boot sector. The action taken by Command AntiVirus in that case is **Report only**.
- If a write-protected diskette or CD-ROM drive has an infected file, that file **cannot** be moved. Command AntiVirus makes a copy of the file and places it in the **Quarantine** folder.
- If a Zip file with multiple infections is quarantined, the number of reported infected files and the number of quarantined files will **not** be the same. This is because the entire Zip file is quarantined.
- If DVP is active, you will be stopped if you try to copy or move an infected file from the **Quarantine** folder.

- If you delete files from the **Quarantine** folder using the Windows delete function, they go to the **Recycled** bin and could be available to reinfect. We recommend that you create a scan task setting the **Action to take** to **Delete**. Then, run a scan on the **Quarantine** folder to delete the infected files completely.

Quarantine Log File

When files have been moved to the quarantine folder, corresponding entries for these files are added to the quarantine log file. This file is named **HISTORY.LOG**. **HISTORY.LOG** is an ASCII text file located in the **Quarantine** folder. You can open it with any text editor.

When a file is moved to the **Quarantine** folder, you need to disinfect or delete it. To do this, you need to check the **HISTORY.LOG** file so that you can determine where the file originated and what it was called before its name was changed. The **HISTORY.LOG** file contains the following columns of information on the infected file:

- **Action** – Specifies what action was performed on the infected file.
- **Computer name** – Specifies the name of the computer that contained the infected file(s).
- **User name** – Specifies the name of the user who was logged into the computer when Command AntiVirus detected the infection. If no one is logged in when the file is quarantined, the user name contains “System.”
- **Date** – Specifies the date that the infection was found.
- **Time** – Specifies the time of day that the infection was found.
- **Quarantine filename** – Specifies the name that was assigned to the infected file when it was moved to the **Quarantine** folder.
- **Original filename** – Specifies the infected file’s original name. This is the name that it had prior to its being moved to the **Quarantine** folder.
- **Message** – Contains a brief message generated by Command AntiVirus describing why the file was moved to **Quarantine** folder.

NOTE: The **HISTORY.LOG** is formatted this way so that you can easily import its contents into most of the popular spreadsheet programs.

The **HISTORY.LOG** file is created when necessary. To clear the log file completely, delete it. It is recreated the next time files are quarantined.

Disinfecting Quarantined Files

You can create a scan task that disinfects infected files that are stored in the quarantine folder.

The new task **must** be an **Administrator Task**.

A user who does **not** have administrator rights can use this task as long as it was created as an **Administrator Task** and access to the **Quarantine** directory is permitted.

To create a task that scans the quarantine folder and disinfects the files that are stored there, follow these steps:

1. From the menu bar, click **Task**. The system displays the drop-down menu.
2. Select **New**. The system displays a **Create New Task** dialog box.
3. In the text box, type a name for your new task, for example:

   ```
   Scan Quarantine Folder
   ```

4. Click **OK**. The system displays the **Select New Task Type** dialog box.
5. Select **Administrator** and click **OK**. The system displays the **Properties** dialog box.
6. Select the drive that contains the **Quarantine** folder, or use the **Browse** button to select the path.
7. Under **File types to scan**, select **All files**.
8. Select the **Scan quarantined files** check box.
9. Under **Action to take**, select **Disinfect**.
10. Click **OK**.

To begin the scan, follow these steps:

1. In the **Task List**, select the scan task that you have just created.
2. Click the **Execute Task** button.

After the files have been disinfected, you **must** rename the files to their original names and move the files back to their original locations. For more information, refer to **Quarantine Log File** located previously in this chapter.

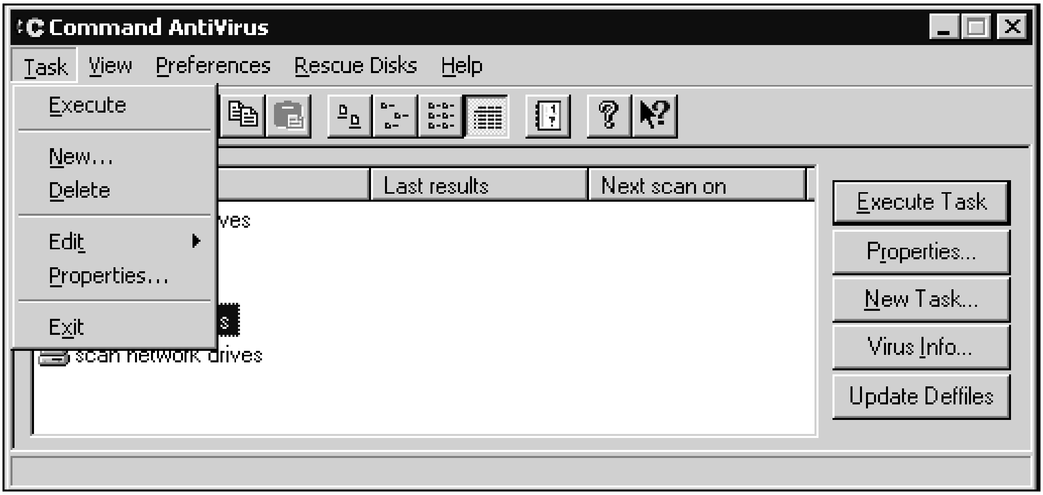
NOTE: If for some reason a file was **not** disinfected and DVP is active, you will be stopped if you try to copy or move an infected file.

If for some reason a file was **not** disinfected and you want to delete the file, we recommend that you create a scan task setting the **Action to take** to **Delete**. Then, run a scan on the **Quarantine** folder to delete the infected file completely.

If you delete files from the **Quarantine** folder using the Windows delete function, they go to the **Recycled** bin and could be available to reinfect.

USING THE TASK MENU

You can access the **Task** menu by clicking **Task** on the menu bar:



Main Dialog Box with Task Menu

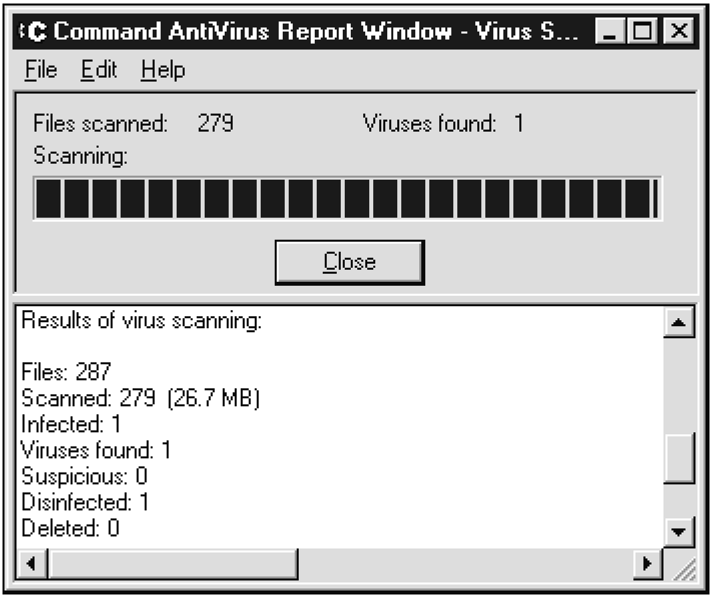
Items on the **Task** menu allow you to:

- **Execute** an on-demand scan task
- Create a **New** scan task
- **Delete** a scan task
- **Edit** an existing scan task.
- Modify the **Properties** of a scan task
- **Exit** the **Command AntiVirus Main** dialog box

EXECUTING A SCAN

To start an on-demand scan, follow these steps:

1. From the **Task List**, select a **Task name**.
2. On the menu bar, click **Task**. The system displays the **Task** menu.
3. Click **Execute**. The scan begins and the system displays a **Command AntiVirus Report Window**. An indicator bar shows the scan's progress. When the scan completes, the window provides details about the scan:



Files scanned: 279   Viruses found: 1
Scanning:

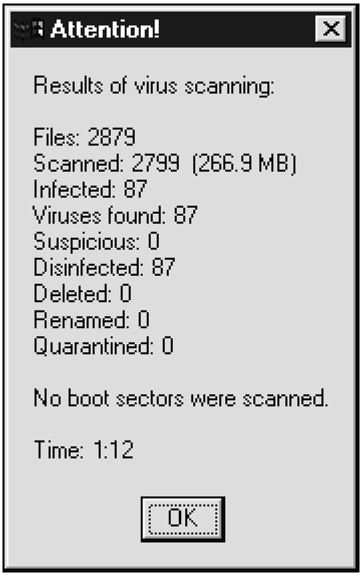
Results of virus scanning:

Files: 287
Scanned: 279 (26.7 MB)
Infected: 1
Viruses found: 1
Suspicious: 0
Disinfected: 1
Deleted: 0

Command AntiVirus Report Window

Use the vertical scroll bar on the right side of the **Command AntiVirus Report Window** to view the entire report. You can use the **File** menu to save a copy of the report, print the report or send a copy of the report through your e-mail system. You can use the **Edit** menu to copy the report to the clipboard and then paste it into another document.

If a virus is found and the **Action to take** is **Report only**, the system displays the **Attention** dialog box to alert you of the infection:



Results of virus scanning:

Files: 2879
Scanned: 2799 (266.9 MB)
Infected: 87
Viruses found: 87
Suspicious: 0
Disinfected: 87
Deleted: 0
Renamed: 0
Quarantined: 0

No boot sectors were scanned.

Time: 1:12

Attention Dialog Box

Click **OK** to close the **Attention** dialog box. Then, if necessary, you can perform an on-demand scan that is set to **Disinfect**.

NOTE: The default setting for **Action to take** in Command AntiVirus is **Report only**. To prompt for disinfection, change the **Action to take** to **Disinfect** or **Disinfect/Query** and allow Command AntiVirus to disinfect the virus.

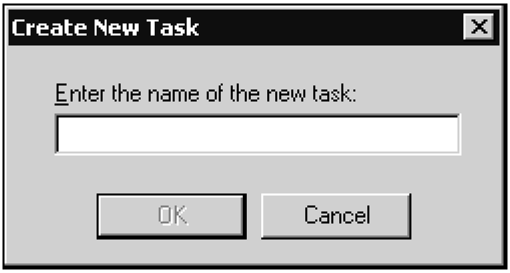
For more information refer to **Configuring Scanning Properties** and **Active Protection** located later in this chapter.

NOTE: You can also start an on-demand scan by selecting a **Task name** and clicking the **Execute Task** button in the **Command AntiVirus Main** dialog box or the **Execute** button on the toolbar.

CREATING A NEW SCAN TASK

To create a new scan task, follow these steps:

1. On the menu bar, click **Task.** The system displays the **Task** menu.
2. Click **New.** The system displays the **Create New Task** dialog box.



Create New Task Dialog Box

3. In the text box, type a name for your new task.

If you are an administrator, the system displays the **Select New Task Type** dialog box. Select the type of task, **User** or **Administrator** and click **OK**.

4. Click **OK**. The system then displays the **Properties** dialog box.

   You can either accept the default settings or customize the settings to your needs. For more information, refer to **Configuring Scanning Properties** located later in this chapter.

NOTE: You can also click the **New Task** button in the **Command AntiVirus Main** dialog box, or you can click the **New** button 🗋 on the toolbar.

DELETING A SCAN TASK

NOTE: If you do **not** have administrator rights, you **cannot** delete an **Administrator Task**.

To delete a scan task, follow these steps:

1. From the **Task List**, select the name of the task that you want to delete.
2. On the menu bar, click **Task.** The system displays the **Task** menu.
3. Click **Delete**.

NOTE: You can also right-click the **Task name** and select **Delete** from the shortcut menu.

EDITING A SCAN TASK

The **Edit** menu item allows you to **Cut**, **Copy**, or **Paste** a selected scan task.

NOTE: If you do **not** have administrator rights, you **cannot** cut an **Administrator Task**.

If you have administrator rights and you copy and paste an **Administrator Task**, the task remains an **Administrator Task**.

If you have user rights and you copy and paste an **Administrator Task**, the task is converted to a **User Task**. It is then subject to the same restrictions that are associated with the assigned permissions.

To copy a scan task, follow these steps:

1. From the **Task List**, select the name of the scan task that you want to copy, for example, **scan hard drives**.
2. On the menu bar, click **Task**. The system displays the **Task** menu.
3. Select **Edit**. The system displays a submenu.
4. Click **Copy**. A copy of the scan task is placed in the clipboard.
5. On the menu bar, click **Task**.
6. Select **Edit**.
7. Click **Paste**. A new scan task named **Copy of scan hard drives** is created in the **Task List**.
8. Right-click the new scan task name. The system displays a drop-down menu.
9. Click **Rename**. A text box opens around the existing name.
10. Type a new name.
11. Press **Enter** to save the change.

Be sure to modify the properties of the new scan task so that it does not duplicate the properties of the task from which it was created. For more information, refer to **Configuring Scanning Properties** located later in this chapter.

You can also use the toolbar buttons to complete different editing tasks:

- The **Cut** button ✂ allows you to delete a selected task and save it to the clipboard. You can then return the task to the **Task List** by clicking the **Paste** button 📋 on the toolbar.
- The **Copy** button allows you to save a copy of a selected task to the clipboard. You can then add the task to the **Task List** by clicking the **Paste** button 📋.
- The **Paste** button 📋 allows you to place a cut or copied task into the **Task List**. The name of the task starts with the phrase “Copy of”. You can then modify and rename the task using the other available options.

CONFIGURING SCANNING PROPERTIES

You can configure the scanning properties of a scan task through the **Properties** dialog box for that task. The **Properties** dialog box can contain the following two dialog boxes. Each of these dialog boxes are identified by a name tab.

- **Properties** – Allows you to modify an existing task and to configure a new task.
- **Schedule** – Allows you to specify when the scan will take place.

This dialog box is available only for an **Administrative Task**.

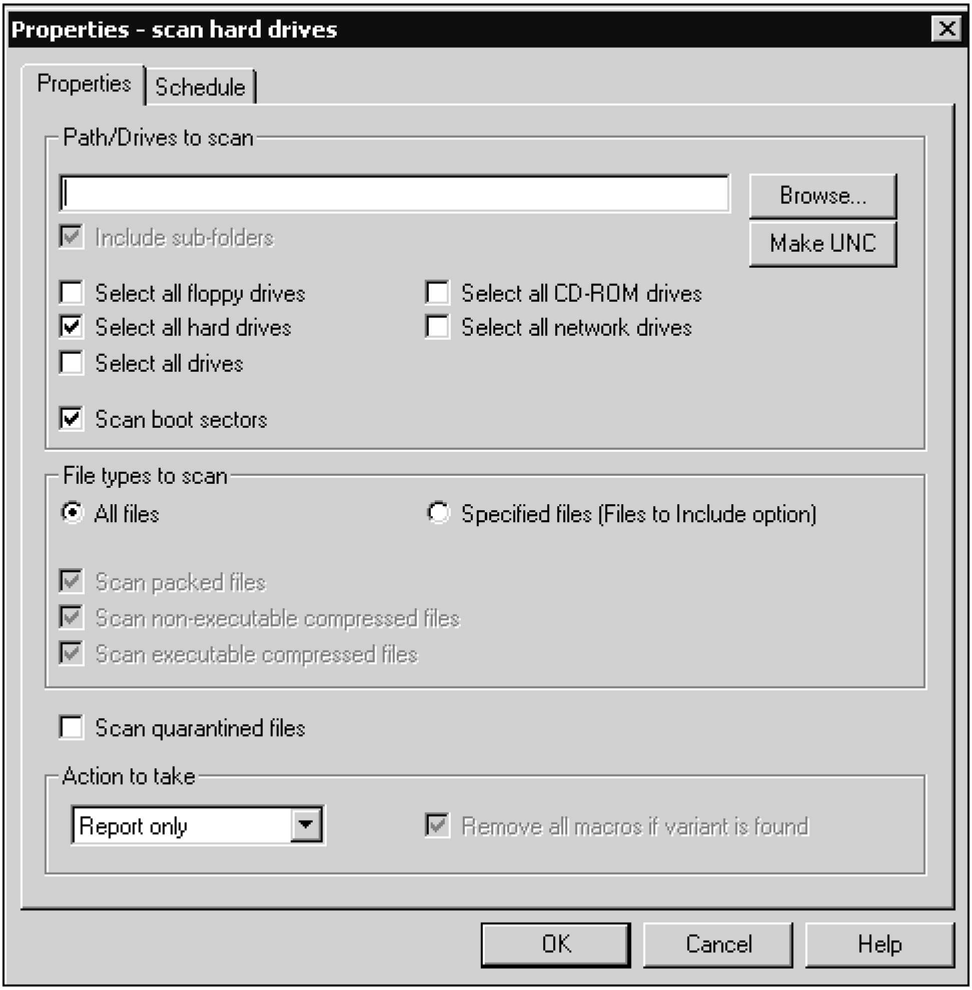
Properties

The **Properties** dialog box allows you to configure the scanning properties of a scan task. In this dialog box you can select the **Paths/Drives to scan**, **File types to scan**, and **Action to take** when a virus is found.

To configure the scanning properties for a scan task, follow these steps:

1. In the **Command AntiVirus Main** dialog box, select a **Task name**.
2. From the menu bar, click **Task**. The system displays the **Task** menu.
3. Click **Properties**. The system displays the **Properties** dialog box.

NOTE: You can also access this dialog box by selecting a **Task name** and clicking the **Properties** button in the **Command AntiVirus Main** dialog box or the **Properties** button on the toolbar.



Path/Drives to scan

☑ Include sub-folders

☐ Select all floppy drives
☑ Select all hard drives
☐ Select all drives
☐ Select all CD-ROM drives
☐ Select all network drives

☑ Scan boot sectors

File types to scan

● All files
○ Specified files (Files to Include option)

☑ Scan packed files
☑ Scan non-executable compressed files
☑ Scan executable compressed files

☐ Scan quarantined files

Action to take

Report only

☑ Remove all macros if variant is found

Properties Dialog Box

4. Under **Drives/paths to scan**, select **one** of the following:

    - **Path** – Use the **Browse** button to select a specific drive or a Universal Naming Convention (UNC) path to scan. For example, you can create a task that performs a scheduled scan on the folder used to store files that are downloaded from other computers.

      When you enter a path in the **Drive/paths to scan** text box, the **Include sub-folders** check box is activated. If you select this option, all subfolders below the path specified are scanned.

    - **Drive(s)** – Select any of the following drives to scan:

        - **Select all floppy drives** – Scans all floppy drives.
        - **Select all hard drives** – Scans all logical hard drives on the local workstation including compressed drives.
        - **Select all drives** – Scans **all** drives to which you have access rights. This option is **not** available for scheduled or inactivity scans.
        - **Select all CD-ROM drives** – Scans all CD-ROM drives.
        - **Select all network drives** – Scans all network drives to which you have access rights and to which you have been mapped. This is **not** available for scheduled or inactivity scans.

5. Under **File types to scan**, select **one** of the following options:

    - **All files** – Scans **all** files including packed, non-executable compressed, and executable compressed files.

We do **not** recommend this option. A scan using **All Files** increases the probability of receiving a false positive from a random string of characters in an otherwise harmless data file. It also takes much longer than using the other scanning options, and it is unlikely to find additional viruses.

- **Specified files** – Scans the default file types. Command AntiVirus contains hard-coded file types that are scanned by default. You can also specify 20 user-defined file types through the **Files to Include/Exclude** dialog box. For more information, refer to **Files to Include/Exclude** located later in this chapter.

NOTE: We recommend this option.

Selecting **Specified files** activates the following check boxes. You can select any of these compressed file options.

- **Packed files** – Scans executable programs that have been compressed with ICE-packed, DIET, LZEXE-packed, PKLITE, and WWPack.
- **Non-executable compressed files** – Scans non-executable files that have been archived using programs such as PKWare's ZIP and ARJ compression utilities.
- **Executable compressed files** – Scans executable files that have been archived using programs such as PKWare's ZIP compression utility.

6. If you want to scan quarantined files, select **Scan quarantined files**. This option allows an administrator to scan the quarantine folder. For more information on the quarantine folder, refer to **Using the Quarantine Feature** located previously in this chapter.

   If **Scan quarantined files** is **not** selected, the quarantine folder will **not** be scanned even if the quarantine directory is in the path.

The **Scan quarantined files** option is available only if you have administrator rights.

NOTE: If the **Action to take** is **Quarantine** or **Quarantine Query**, **Scan quarantined files** is unavailable as you **cannot** quarantine files that are already in the quarantine directory.

7. Under **Action to take**, click the drop-down arrow. The system displays a drop-down list.
8. Select **one** of the following actions to take when a virus is found:

   - **Report only** – Informs you when a virus is detected. No other action is taken. For example, you can select this option to verify the type of virus before disinfecting it.

NOTE: This option is the default for all new scans and for all of the preset scans provided by Command AntiVirus. You may want to change this setting after becoming more familiar with the software.

- **Disinfect** – Disinfects files automatically. If disinfection is not possible, Command AntiVirus asks if you want to delete the file.

  Selecting this option activates the **Remove all macros if variant is found** check box. Select this check box to remove all macros from any file containing a new or modified variant of a macro virus.

NOTE: If the **Action to take** is **Disinfect** or **Disinfect/Query** and the **Remove all macros if variant is found** check box is **not** selected, files that contain remnants or are variants of macro infections are renamed.

- **Disinfect/Query** – Identifies a virus and asks if you want to disinfect it.

  Selecting this option activates the **Remove all macros if variant is found** check box. Select this check box to remove all macros from any file containing a new or modified variant of a macro virus.

NOTE: If the **Action to take** is **Disinfect** or **Disinfect/Query** and the **Remove all macros if variant is found** check box is **not** selected, files that contain remnants or are variants of macro infections are renamed.

- **Delete** – Deletes infected files automatically.

With **Delete**, the potential exists for data loss. Some rare viruses are able to perform encryption on the hard drive, making file recovery difficult.

- **Delete/Query** – Identifies a virus and asks if you want to delete the infected file.

- **Rename** – Automatically provides a new non-executable name for an infected file by putting a “V” in place of the first letter of the extension. For example, .COM becomes .VOM and .EXE becomes .VXE.
- **Rename/Query** – Identifies a virus-infected file and asks if you want to rename it. If you choose **Yes,** it renames the file as previously described. If you choose **No**, you need to disinfect or delete the file.
- **Quarantine** – Places an infected file in a secure location for evaluation, disinfection or deletion at a later time.

This option is available only to administrators.

- **Quarantine/Query** – Prompts you before quarantining a file.

This option is available only to administrators.

Query is **<u>not</u>** available in scheduled or inactivity scans as these scans usually need to occur unattended. Therefore, if the **Action to take** for a scan task was set to **Disinfect/Query**, the action would change to **Disinfect**.

Quarantine/Query would change to **Quarantine** and so on. A warning message displays to remind you of this.

9. Click **OK**.

Schedule

This dialog box is available only for an **Administrator Task**.

The **Schedule** dialog box allows you to specify when a scan will take place.

Scheduled scans can be a very useful anti-virus tool. Administrators can create scheduled scans that are installed on each user’s computer. Scheduling a daily scan guarantees that a user's workstation is consistently checked for viruses. Scheduled scans run as long as the computer is on even if no one is logged onto the computer.

Command AntiVirus does **not** need to be opened for a scheduled scan to take place. Administrator-defined scheduled scans run even when no one is logged onto the machine. When a scheduled scan begins, a small clock with moving hands appears over the yellow **C** icon in the system tray. If the computer is **not** on when a scan is scheduled to run, the scan is skipped.

Scheduling is controlled by a service named CSS AV Scheduler (CSS-AVS.EXE). This service runs in the background and is activated on startup. It is necessary to have this service started for scheduled scans to take place.

NOTE: Activity performed by CSS AV Scheduler can be seen in the Windows **Event Viewer Application Log**. You can view Event Viewer from the **View** menu of Command AntiVirus or by right-clicking the yellow **C** icon in the system tray.

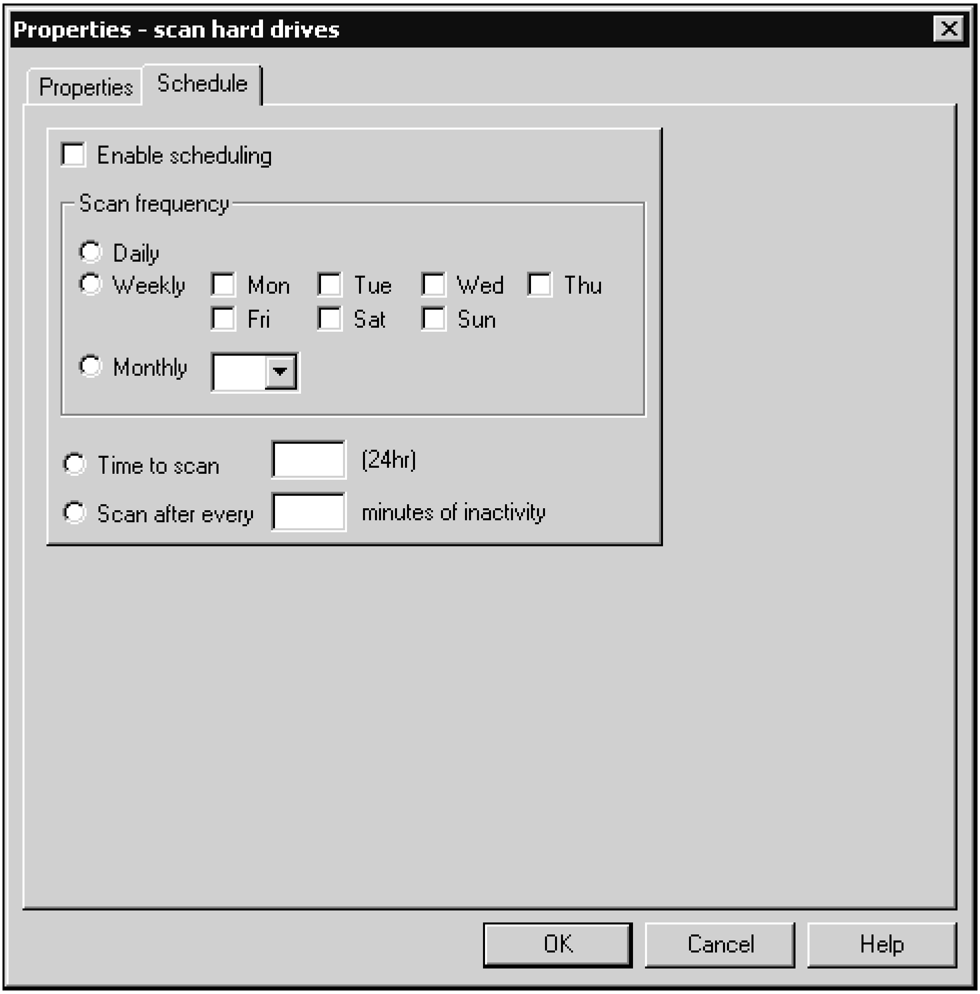
The Event Viewer log may become filled if Command AntiVirus encounters a large number of infected files. If that happens frequently, you might consider increasing the **Maximum Log Size** in Event Viewer. Consult your operating system’s manual for furtherinformation.

To schedule a scan, follow these steps:

1. In the **Command AntiVirus Main** dialog box, select a **Task name**.
2. From the menu bar, click **Task**. The system displays the **Task** menu.
3. Click **Properties**. The system displays the **Properties** dialog box.

NOTE: You can also access this dialog box by selecting a **Task name** and clicking the **Properties** button in the **Command AntiVirus Main** dialog box or the **Properties** button 🗔 on the toolbar.

4. Click **Schedule**. The system displays the **Schedule** dialog box:



Properties - scan hard drives

□ Enable scheduling

Scan frequency

○ Daily

○ Weekly □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

○ Monthly

○ Time to scan (24hr)

○ Scan after every minutes of inactivity

Schedule Dialog Box

5. Select the **Enable scheduling** check box.

Checking this box turns on scheduled scanning. If the box is **not** checked, scheduled scans will **not** take place.

6. Under **Scan Frequency**, select **one** of the following options:

- **Daily** – Scans each day.
- **Weekly** – When you select this option, you can then select the day or days each week that you want a scan to take place.
- **Monthly** – When you select this option, you can then select from the drop-down list the day of the month that you want the scan to take place.

7. Select **one** of the following options:

- **Time to scan** – Allows you to enter the time of day that you want the scan to start. Using a 24-hour format with “00.00” indicating midnight, enter the time of day in the text box. For example, if you want to scan at 1:30 p.m., enter 13:30.

NOTE: If the computer is **not** on when a scan is scheduled to start, the scan is skipped.

If you would like to schedule an immediate scheduled scan for testing purposes, the scan should be scheduled at least five minutes ahead of the current time.

- **Scan after inactivity** – Allows you to specify a period of keyboard or mouse inactivity that must pass before the scan starts.

NOTE: A user **must** be logged on and F-AGENT **must** be running for a scan after inactivity to take place.

If the inactivity scan time is too small, you can run into a perpetual scan situation.

To stop a scheduled scan that is running, follow these steps:

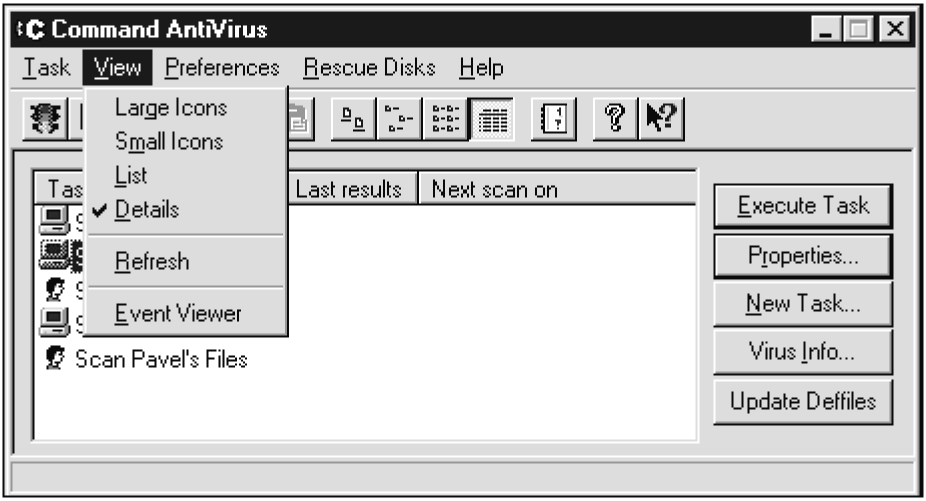
To stop a scheduled scan, you must have administrator rights.

1. On the Windows taskbar, click the **Start** button.
2. Select **Settings**.
3. Select **Control Panel**.
4. Select **Administrative Tools**.
5. Click **Services**. The system displays the **Services** console.
6. From the left pane, select **CSS Scheduler**.
7. On the menu bar, click **Action**. The system displays a drop-down menu.
8. Click **Stop**.

To start the service so that scheduled scans are active again, repeat **Steps 1** through **7** and then click **Start**.

USING THE VIEW MENU

You can access the **View** menu by clicking **View** on the menu bar:



Main Dialog Box with View Menu

The **View** menu allows you to change the way you view the scan tasks shown in the **Task List**. The available menu items are described briefly. For more information, refer to your operating system's manual.

LARGE ICONS

Selecting this menu item displays the **Task List** as large icons with the scan task name located below each icon.

To select this view, you can also click the **Large Icons** button on the toolbar.

SMALL ICONS

Selecting this menu item displays the **Task List** as several columns of small icons with the scan task name located to the right of each icon.

To select this view, you can also click the **Small Icons** button on the toolbar.

LIST

Selecting this menu item displays the **Task List** as a single column of small icons with the scan task name located to the right of each icon.

To select this view, you can also click the **List** button on the toolbar.

DETAILS

Selecting this menu item displays the **Task List** with three column headers: **Task name**, **Last results**, and **Next scan on**.

The **Task name** column contains small icons with the scan task name located to the right of each icon. The **Last results** column contains the results of the last scan if a virus was found. The **Next scan on** column contains the time of the next scheduled scan. This is the only viewing option that displays column headers.

To select this view, you can also click the **Details** button on the toolbar.

REFRESH

Selecting this menu item updates the **Task Window** to reflect Command AntiVirus task information stored on the disk. This is useful when copying task files from the network.

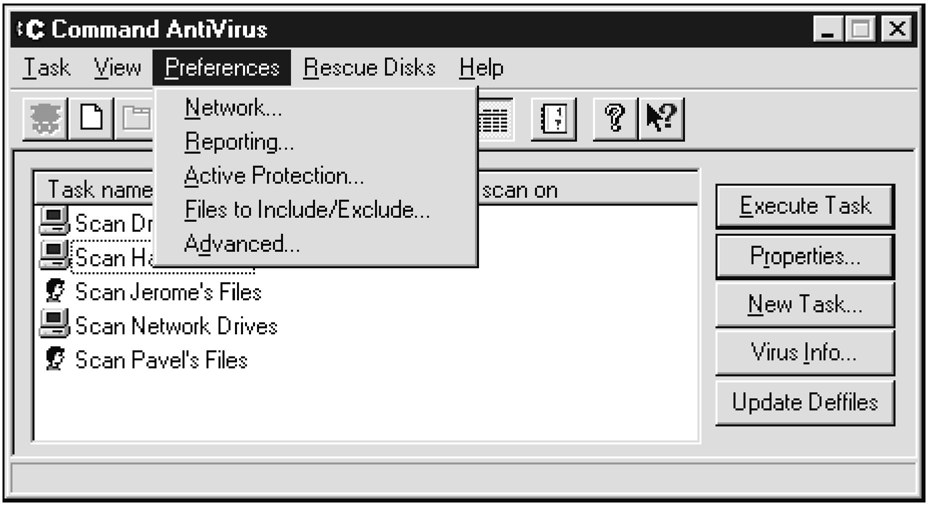
EVENT VIEWER

Selecting this menu item allows you to access the Windows Event Viewer.

To access Event Viewer, you can also click the Event Viewer button on the toolbar. For more information about Event Viewer, refer to **Locating Scan Results in Event Viewer** located previously in this chapter.

USING THE PREFERENCES MENU

The **Preferences** menu is one of the key areas for customizing Command AntiVirus. You can access this menu by clicking **Preferences** on the menu bar.



Preferences Menu

The **Preferences** menu contains the following items:

- **Network** – Allows you to set up messaging through your e-mail system and central event logging if you are running our companion product, Command AntiVirus for NetWare.
- **Reporting** – Allows you to decide on available options for virus notification.
- **Active Protection** – Allows you to enable, disable or configure on-access protection. You can also set the action that Command AntiVirus takes when it detects a virus.
- **Files to Include/Exclude –** Allows you to specify additional file types to **Include in** and what files and/or directories to **Exclude** from all scans.
- **Advanced –** This menu item is available only if you are a member of the local Administrators group.

The Advanced menu item allows you to set the path to the **automatic update directory**, and update an individual workstation on demand by using the **Update Now** button. You can also set the update sites that are accessed by the **Update Deffiles** button, change the quarantine folder, receive a warning if the definition files are out of date, and change the folder containing the Command AntiVirus **Administrator Task** files.

All of the above-mentioned features are described in detail in the following sections.

NETWORK

When you select **Network** from the **Preferences menu**, the system displays the **Network** dialog box. The **Network** dialog box **can** contain two dialog boxes. Each of these dialog boxes is identified by a named tab.

If you installed **Netware Reporting**, the **NetWare** dialog box allows you to configure scan options that are designed to work with Command AntiVirus for NetWare. The **Messaging** dialog box allows you to set up messaging to your network.

NetWare

NOTE: This dialog box is **not** visible if **NetWare Reporting** is **not** installed and running.

Through the **NetWare** dialog box, you can configure scan options that are designed to work with Command AntiVirus for NetWare.

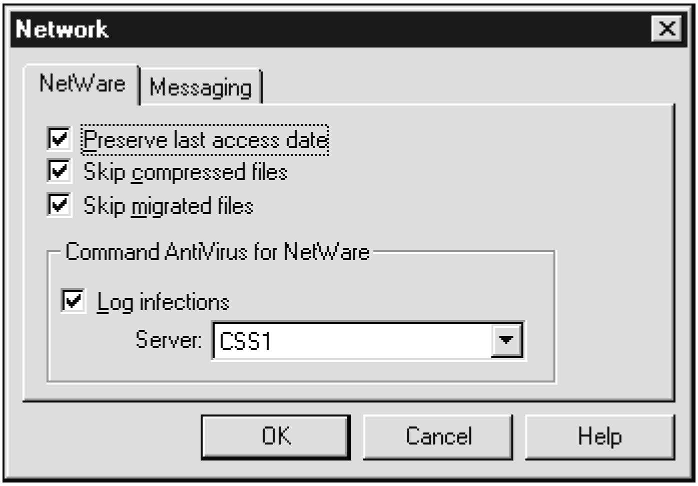
NetWare Reporting allows the workstation to communicate to a server that is running Command AntiVirus for NetWare, and it records any virus incidents to the F-PROT log and the AlertTrack™ log. **NetWare Reporting** also preserves the last access date and allows compressed and migrated files to be skipped during a network scan.

The **NetWare Reporting** feature is installed to the Program Files\Common Files\Command Software\NetWare directory only if you select this feature prior to the installation of Command AntiVirus. For more information, refer to **Customizing Your Installation Settings** in the ***Network Administration*** chapter.

If you are not running NetWare or Command AntiVirus for NetWare, it is not necessary or advisable to install **NetWare Reporting**.

To configure the NetWare options, follow these steps:

1. From the Command AntiVirus menu bar, click **Preferences**. The system displays a drop-down menu.
2. Click **Network**. The system displays the **Network** dialog box.
3. Click the **NetWare** tab. The system displays the **NetWare** dialog box:



☑ Preserve last access date
☑ Skip compressed files
☑ Skip migrated files

Command AntiVirus for NetWare

☑ Log infections

Server: CSS1

Netware Dialog Box

4. Select any of the following options:

- **Preserve last access date** – Prevents the modification of the last access date on the file.

  Many archiving programs reference the last access date to determine if a file is eligible for archiving. If this option is **not** selected, the last access date will be updated to show the last time Command AntiVirus scanned the file.

Use this option with caution. If you do **not** select this option, you could prevent archiving software from functioning properly.

- **Skip compressed files** – Does **not** scan compressed files.

  Compressed files are usually files that have not been accessed for a period of time, perhaps weeks or months. If the file was compressed after an initial scan with Command AntiVirus, it is unlikely that it contains a virus.

  You can shorten scan times by selecting this option. We recommend that you scan compressed files once when Command AntiVirus is first installed and then again with every major scan update.

- **Skip migrated files** – Does **not** scan migrated files.

  As migrated files are, by definition, not in use, you can shorten scan times by selecting this option. We recommend that you scan migrated files once when Command AntiVirus is first installed and then again before using them.

- **Log infections** – If you are running Command AntiVirus for NetWare, logs detected viruses to a Command AntiVirus for NetWare log and an AlertTrack log.

  Select a valid server name from the **Server** drop-down list. If a virus is found, it is added to that server's log file. To view the log, use a text editor or the **View** option in the **Command AntiVirus for NetWare Administration Main** dialog box.

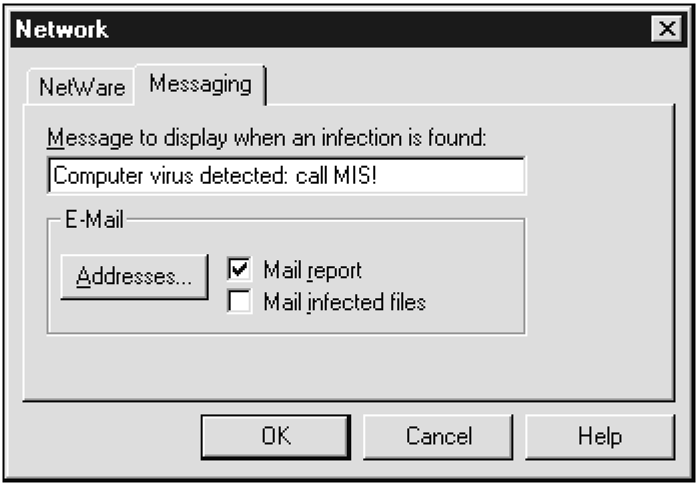
5. Click **OK**.

Messaging

Through the **Messaging** dialog box, you can modify the message that is shown to users when a virus is detected. You can also control notification using your existing MAPI (Messaging Application Programming Interfaces) e-mail system.

To configure the messaging options, follow these steps:

1. From the Command AntiVirus menu bar, click **Preferences**. The system displays a drop-down menu.
2. Click **Network**. The system displays the **Network** dialog box.
3. Click the **Messaging** tab. The system displays the **Messaging** dialog box:



Network

NetWare | Messaging

Message to display when an infection is found:

Computer virus detected: call MIS!

E-Mail

☑ Mail report

□ Mail infected files

Messaging Dialog Box

4. In the **Message to display when an infection is found** text box, type a message that will be shown to users when a virus is detected.

   You can enter a text message of up to 80 characters in length.

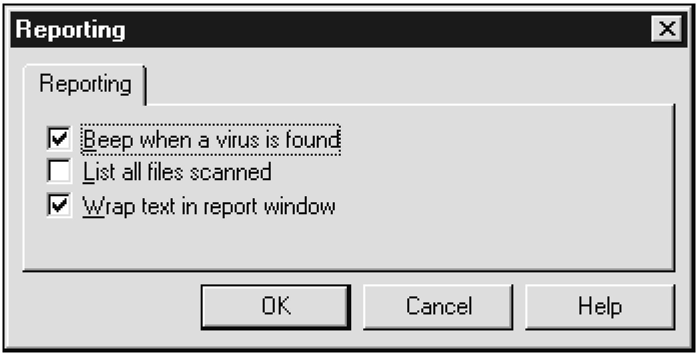
5. Click **Addresses** to select who receives the messages.
6. Select any of the following options:
   - **Mail report** – Mails a virus report to the person(s) selected in **Addresses**.
   - **Mail infected files** – Mails the infected file to the address(es) selected in **Addresses**.
7. Click **OK**.

REPORTING

Through the **Reporting** dialog box you can control how the scan results for a manual scan are displayed for reporting purposes. You can also select an audible virus warning.

To configure the reporting options for a manual scan, follow these steps:

1. From the Command AntiVirus menu bar, click **Preferences**. The system displays a drop-down menu.
2. Click **Reporting**. The system displays the **Reporting** dialog box:



☑ Beep when a virus is found
☐ List all files scanned
☑ Wrap text in report window

Reporting Dialog Box

3. Select any of the following options:
   - **Beep when a virus is found** – The PC speaker emits a short beep when a virus is detected.
   - **List all files scanned** – Verifies that the appropriate files are being scanned. You can avoid lengthy reports by clearing this option.
   - **Wrap Text In Report Window** – Selecting this option may make it easier to read short reports. In longer reports, you may find it easier to find individual file listings without wrapping the text.
4. Click **OK**.

ACTIVE PROTECTION

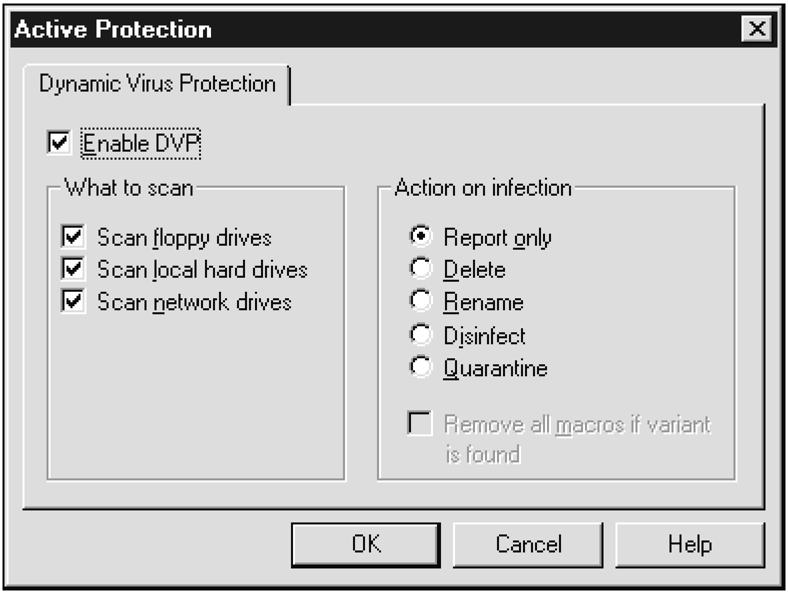
On-access scanning is an important element of protection. It prevents your system from becoming infected between full scans. This on-access protection is provided through Dynamic Virus Protection (DVP).

DVP provides transparent, real-time scans of each program that is 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 scanned automatically. DVP also scans files that are opened in a DOS window.

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 when a virus is found.

To enable or disable DVP or change the active protection options, follow these steps:

1. From the Command AntiVirus menu bar, click **Preferences**. The system displays a drop-down menu.
2. Click **Active Protection**. The system displays the **Active Protection** dialog box.



Active Protection

Dynamic Virus Protection

☑ Enable DVP

What to scan

☑ Scan floppy drives
☑ Scan local hard drives
☑ Scan network drives

Action on infection

● Report only
○ Delete
○ Rename
○ Disinfect
○ Quarantine

□ Remove all macros if variant is found

Active Protection Dialog Box

3. Select or clear the **Enable DVP** check box.

   This check box **<u>must</u>** be selected for on-access protection to work. We highly recommend that you select this option. This option is selected by default.

   If you are disabling DVP, proceed to **Step 6**.

4. Under **What to scan**, select the drive(s) that you want to scan.

   Enabling DVP activates this option. You can then select which types of drives will be covered by DVP’s on-access protection when files are accessed:

   - Scan floppy drives – Includes CD-ROM drives.
   - Scan local hard drives
   - Scan network drives

5. Under **Action on infection**, select any **<u>one</u>** of the following actions to take when a virus is found.

NOTE: Some networks may not allow certain actions. If this is the case, a notification will be sent indicating the constraint.

- **Report only** – Informs you when a virus is detected. No other action is taken other than to deny access to the file. Select the **Report only** option if you want to verify the type of virus before disinfection. This option is selected by default.
- **Delete** – Automatically deletes virus-infected files.

While this is a powerful option, the potential exists for data loss. Some rare viruses perform encryption on the hard drive making file recovery difficult.

- **Rename** – Automatically adds a **.INFECTED** to the original file name and extension of the infected file. For example, **EICAR.COM** becomes **EICAR.COM.INFECTED**.
- **Disinfect** – Automatically disinfects virus-infected files.

  Selecting this option activates the **Remove all macros if variant is found** check box. Select this check box to remove all macros from any file containing a new or modified variant of a macro virus.

NOTE: If the **Action to take** is **Disinfect** and the **Remove all macros if variant is found** check box is **<u>not</u>** selected, files that contain remnants or are variants of macro infections are renamed.

While **Disinfect** is a powerful option, the potential exists for data loss. Some rare viruses perform encryption on the hard drive making file recovery difficult.

- **Quarantine** – Moves an infected file to a separate directory so that the file can be evaluated, disinfected or deleted at a later time. If the quarantine directory does not have enough room to store the infected file, the file will not be moved into that directory. Instead, the file will only be reported by Command AntiVirus.

6. Click **OK** to save your changes.

FILES TO INCLUDE/EXCLUDE

The **Files to Include/Exclude** dialog box allows you to specify additional file types to **Include** in and what files and /or directories to **Exclude** from all scans.

This dialog box contains three dialog boxes: **Files to Include**, **Files to Exclude** and **Directories to Exclude**. Just click the tab of the option that you want to modify, for example, **Files to Exclude**. The system displays the corresponding dialog box.

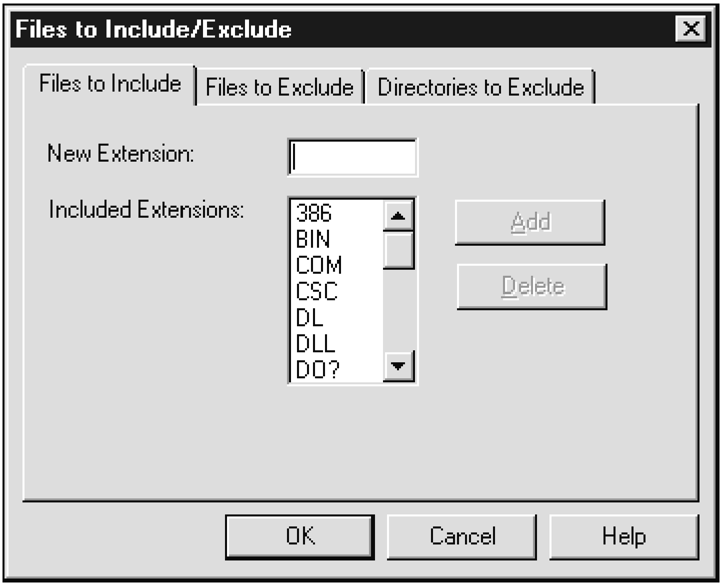
NOTE: For the changes that you make to take effect immediately, you **must** disable Dynamic Virus Protection (DVP) and then enable it. Otherwise, the changes will take effect the next time you start your computer.

To disable or enable DVP, click **Preferences**, **Active Protection.** The system displays the Dynamic Virus Protection dialog box. To disable DVP, remove the check mark in the **Enable DVP** check box and click **OK**. To enable DVP, add the check mark to the **Enable DVP** check box and click **OK**.

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

Files to Include

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



Included Extensions: 386 BIN COM CSC DL DLL DO?

Files to Include Dialog Box

To exclude a hard-coded file type from scans, add an asterisk and the file type's extension to the **Excluded 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 **<u>not</u>** scanned.

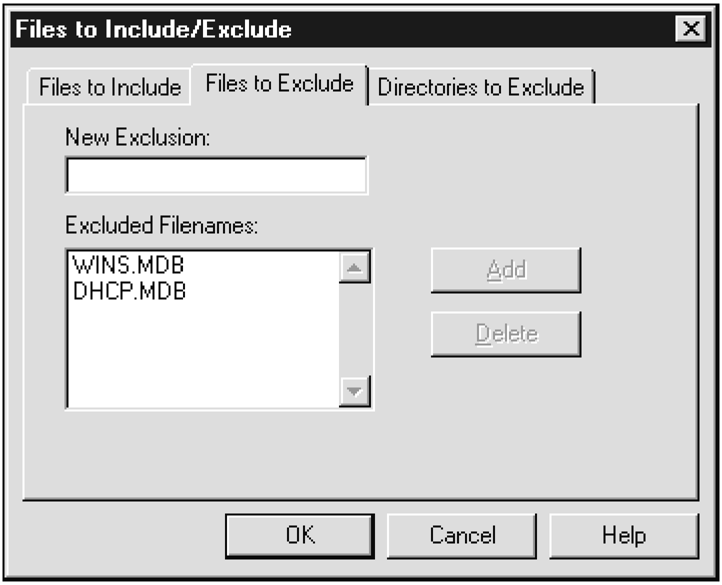
This option also allows you to specify **20** user-defined file types for CSAV to scan. To add a file name extension to the list, type the extension in the **New Extension** text box and click **Add**. To remove an extension that you have added, select the extension and click **Delete**.

NOTE: Command AntiVirus does **<u>not</u>** 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 or scheduled scan of **Packed Files** during off-peak hours. To scan self-extracting and packed files, select the **Packed Files** check box in the **Properties** dialog box.

Files to Exclude

This option allows you to specify which files CSAV does **not** scan. The files that are excluded from the scan are displayed in the **Excluded Filenames** list.



Excluded Filenames:
WINS.MDB
DHCP.MDB

Files to Exclude Dialog Box

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

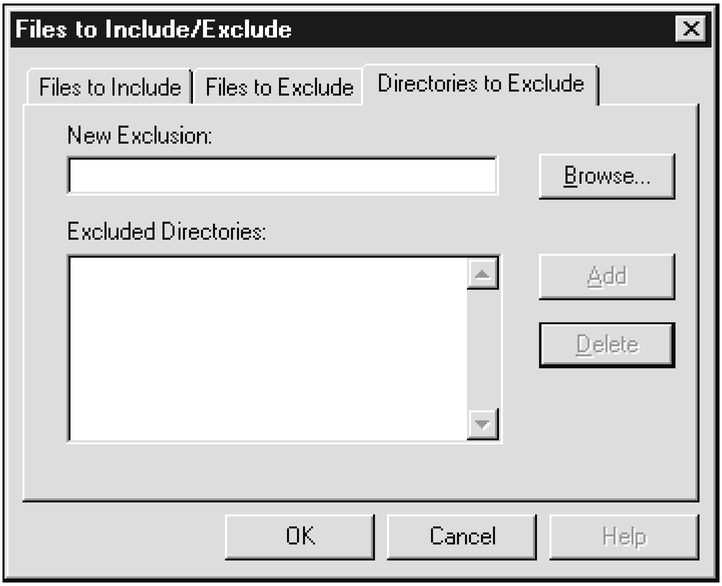
```
abc*
```

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 **Excluded 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.

Directories to Exclude

This option allows you to specify which directories CSAV does **not** scan. The directories that are excluded from the scan display in the **Excluded Directories** list.



Directories to Exclude Dialog Box

NOTE: The **Directories to Exclude** option has priority over the **Files to Include** and the **Files to Exclude** options. For example, **all** files in the excluded directory and its subdirectories are **not** scanned even if the file extensions are included in the **Included Extensions** list.

To add a directory to the list, type the directory name in the **New Exclusion** text box and click **Add**. To remove a directory, select the directory and click **Delete.**

NOTE: You can also use **Browse** to locate the directory. The system displays the **Open** dialog box. Select the directory and click **OK**.

ADVANCED

This menu item is available only if you are a member of the local Administrators group.

When you select **Advanced** from the **Properties** menu, the system displays the **Advanced** dialog box. This dialog box contains the following dialog boxes. Each of these dialog boxes is identified by a name tab.

- **Automatic Update** – Allows you to set the path to the **automatic update directory** and update an individual workstation on demand by using the **Update Now** button. For more information, refer to **Automatic Update** in the ***Network Administration*** chapter.
- **Update Deffiles Now** – Allows you to set the update sites that are accessed by the **Update Deffiles** button. For more information, refer to **Definition Files Update Button** in the ***Network Administration*** chapter.
- **Quarantine Path** – Allows you to specify the path of a quarantine folder other than the default folder. For more information, refer to **Changing the Quarantine Folder** in the ***Network Administration*** chapter.
- **Miscellaneous** – Allows you to receive a warning if the definition files are out of date. For more information, refer to **Setting a Definition Files Warning** in the ***Network Administration*** chapter.

- **Task Path** – Allows you to specify the path of a folder other than the default folder that contains the Command AntiVirus system scan task files. For more information, refer to **Changing the System Scan Task Folder** in the ***Network Administration*** chapter.

RESCUE DISKS

To create a rescue disk set, you **must** be a member of the local Administrators group.

If you did not choose to make a Command AntiVirus rescue disk during installation, you can create one from the **Rescue Disks** menu on the menu bar.

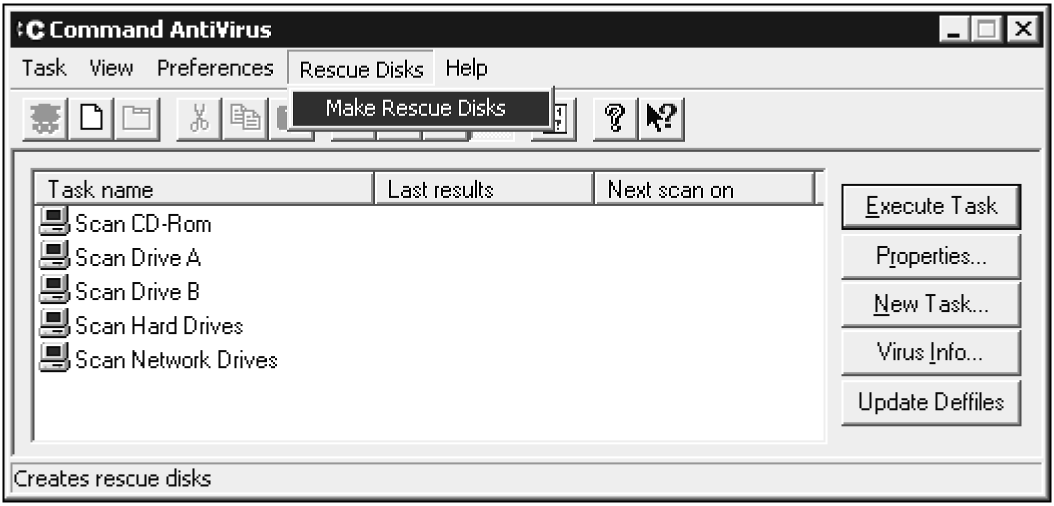
NOTE: To create a rescue disk set, you will need three blank, formatted 1.44MB diskettes labeled **CSAV Rescue Disk 1 for (User's Computer ID)**, **CSAV Rescue Disk 2 for (User's Computer ID)**, and **CSAV Rescue Disk 3 for (User's Computer ID)**. Also, make sure that the diskettes and your system are **virus-free**.

For NTFS systems, unless you can access an NTFS drive from within DOS, for example, by using third-party software, you will **not** be able to use the rescue disk set to scan files on an NTFS drive.

You can use **Rescue Disk 1** on NTFS systems at any time to repair damaged or infected boot sector information.

To create a rescue disk set, follow these steps:

1. On the menu bar, click **Rescue Disks**. The system displays the drop-down menu:

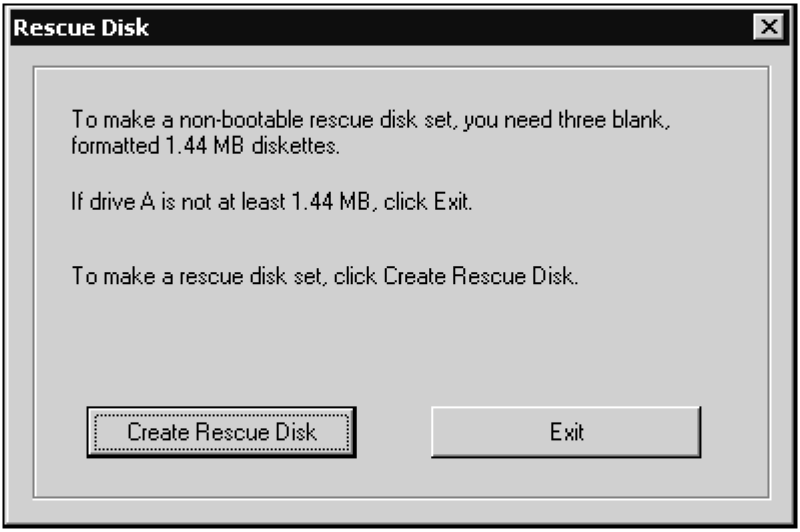


Task name	Last results	Next scan on
Scan CD-Rom		
Scan Drive A		
Scan Drive B		
Scan Hard Drives		
Scan Network Drives		

Creates rescue disks

Make Rescue Disks

2. Click **Make Rescue Disks**. The system displays the **Rescue Disk** dialog box:



To make a non-bootable rescue disk set, you need three blank, formatted 1.44 MB diskettes.

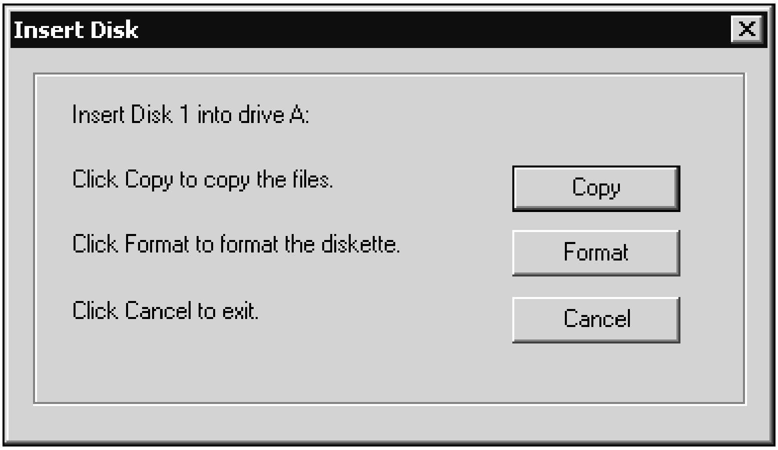
If drive A is not at least 1.44 MB, click Exit.

To make a rescue disk set, click Create Rescue Disk.

Rescue Disk Dialog Box

NOTE: If drive A is not at least 1.44 MB, or you do not want to create a rescue disk set, click **Exit**.

3. To make a non-bootable rescue disk set, click **Create Rescue Disk**. The system displays the **Insert Disk** dialog box:



Insert Disk

Insert Disk 1 into drive A:

Click Copy to copy the files.

Click Format to format the diskette.

Click Cancel to exit.

Insert Disk Dialog Box

4. Insert **Disk 1** into drive A and click **Copy**. The system returns to the **Rescue Disk** dialog box which displays the files being copied.

   To format a diskette, click **Format**. Then, continue with the formatting process. When the formatting process is complete, click **Close** to return to the **Insert Disk** dialog box.

5. When the copying is complete, the system displays a dialog box informing you that the rescue disk was created successfully. Click **OK** to continue. The system displays the **Insert Disk** dialog box

6. Remove **Disk 1** from drive A, and set the write-protect tab to prevent any modifications.

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

7. Insert **Disk 2** into drive A and click **Copy**. The system returns to the **Rescue Disk** dialog box which displays the files being copied.

8. When the copying is complete, the system displays a dialog box informing you that the rescue disk was created successfully. Click **OK** to continue. The system returns to the **Rescue Disk** dialog box.
9. Remove **Disk 2** from drive A, and set the write-protect tab to prevent any modifications.
10. Insert **Disk 3** into drive A and click **Copy**. The system returns to the **Rescue Disk** dialog box which displays the files being copied.
11. When the copying is complete, the system displays a dialog box informing you that the rescue disk was created successfully. Click **OK** to continue. The system returns to the **Rescue Disk** dialog box.
12. Remove **Disk 3** from drive A, and set the write-protect tab to prevent any modifications.
13. Click **Exit**. The system returns to the **CSAV Main** dialog box.

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 on only the computer that was used to create the file.

USING COMMAND ANTIVIRUS

TESTING THE RESCUE DISK SET

To test 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
```

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.

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

USING THE RESCUE DISK SET

Dealing with some viruses may require the use of your rescue disk set. The rescue disk process involves two phases.

The first phase focuses on recovery by detecting and removing any executable, boot sector, and MBR-infecting viruses that inhibit or prevent system startup.

After successful recovery, the second phase focuses on scanning and disinfecting all remaining virus-infected files, for example, macro virus-infected files.

To assure a successful rescue, you **must** perform both phases.

To perform Phase One, 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
```

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.
11. Proceed to **Phase Two**.

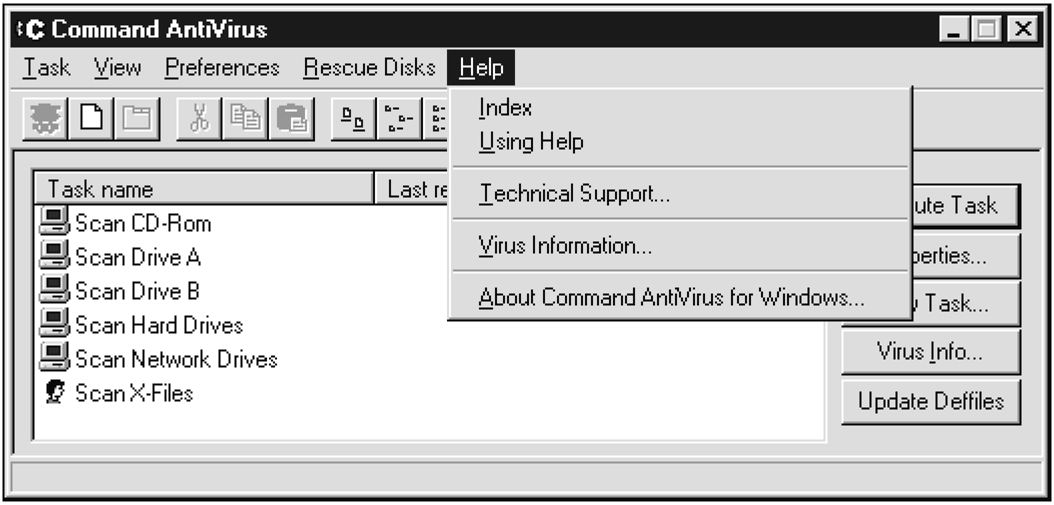
To perform Phase Two, follow these steps:

1. Restart your computer as normal.
2. Use Command AntiVirus to perform a scan of your local hard drives. This scan detects and disinfects any remaining virus-infected files on your computer.

After completing the **Phase Two** scan, you can return to computing as normal.

HELP MENU

The **Help** menu provides general help for Command AntiVirus. You can access this menu by clicking **Help** on the Command AntiVirus menu bar.



Help Menu

INDEX

This menu item allows you to access the **Help** file **Index** dialog box. This dialog box contains an alphabetical list of help topics that you can display.

USING HELP

This menu item gives basic instructions for using the help system.

TECHNICAL SUPPORT

This menu item provides telephone numbers and other information on contacting your local technical support representative.

VIRUS INFORMATION

This menu item provides a listing of all the viruses and virus variants that are handled by Command AntiVirus. The list is generated directly from the Command AntiVirus definition files that are on your computer.

ABOUT COMMAND ANTIVIRUS FOR WINDOWS NT/2000

This menu item provides the following information:

- Product version number
- Date of the scan engine
- Date of the SIGN.DEF definition file
- Date of the MACRO.DEF definition file
- Copyright information

You can also access this information by clicking the question mark button on the Command AntiVirus toolbar.

BOOT RECORD SUPPORT

The Master Boot Record (MBR) is an important part of your hard drive. To help you fix a damaged or virus-infected MBR, Command AntiVirus provides you with two special programs: FIXDSKNT.EXE and FIXDISK.EXE. Both of these command-line utilities work together to remove unknown boot sector viruses safely. They also allow you to create a virus data file. This file can be used at a later date for analysis and, if necessary, data recovery.

FIXDSKNT.EXE

FIXDSKNT.EXE saves the first track of the hard disk to a data file. If this file is created before a virus infection, it can be used as a rescue file should your boot record or MBR later become infected.

If you encounter a new boot virus that cannot be disinfected, FIXDSKNT.EXE can also be used to save a copy of your infected boot record. This copy can then be sent to our development team for analysis and can be used for updating Command AntiVirus.

USING FIXDSKNT TO CREATE A RESCUE FILE

FIXDSKNT.EXE produces a rescue file containing an image of the MBRs and the boot sectors of all physical hard drives. By default, the rescue file created by FIXDSKNT.EXE is called RESCUE.DAT. However, if you want, you can specify a different file name for it.

In Command AntiVirus for Windows NT®/2000 and Command AntiVirus for Windows NT®, to create a rescue file, you must be a member of the local Administrators group.

To use the FIXDSKNT utility to create a rescue file, follow these steps:

1. On your hard drive, change to the directory that contains FIXDSKNT.EXE. This is the directory that contains the Command AntiVirus program files.
2. Insert a virus-free, blank formatted diskette into drive A.

NOTE: If you prefer, you can save your rescue file to an MS-DOS system diskette. This would provide the additional ease-of-use of having a bootable diskette that contains your computer's Command AntiVirus rescue file.

3. Type the following command:

```
FIXDSKNT A:
```

This writes the rescue file, RESCUE.DAT, to the diskette in drive A. If you would like to save the rescue file under a different name, add that name to the above-mentioned command. For example, to create a rescue file called TEST.DAT type:

```
FIXDSKNT A:TEST.DAT
```

This stores a rescue file called TEST.DAT onto the diskette in drive A.

4. Remove the diskette from drive A, and set the write-protect tab to prevent any modifications. Label the diskette "Boot Record/MBR File for XXX". Be sure to substitute the "XXX" notation with a word or phrase that identifies the computer on which you made the rescue file. Store the diskette in a safe place.

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

Should you ever need to use the rescue file that you have created on your diskette, it can be moved back to your computer by using the FIXDISK.EXE utility (not to be confused with the FIXDSKNT utility mentioned in the preceding instructions). The following section provides details on how to use FIXDISK.EXE.

FIXDISK COMMAND-LINE OPTIONS

To use FIXDISK.EXE, you must start your computer from a DOS system disk.

FIXDISK.EXE is a 16-bit program that can be used to replace an image of the boot area or repair the boot record of your computer. FIXDISK.EXE can attempt a generic repair or, if you have a previously saved rescue file, it can replace your damaged or infected boot area with that file, allowing you to continue your computing as normal.

To use FIXDISK.EXE, on your hard drive, change to the directory that contains FIXDISK.EXE. This is the directory that contains the Command AntiVirus program files.

To display a list of command-line options, type **FIXDISK** and press **Enter**.

Table 2: FIXDISK.EXE Command Line Options

Switch	Description
REPAIR	Saves the first track and attempts a repair of the boot area.
SAVE	Takes an image of the boot area and backs up the first track to a file.
UNDO	Restores the boot area to its original state before repair.
FIND	Searches drive for a rescue file.
RESCUE	Used with the following switch for restoring a rescue file: RESTORE Restores the file that was previously saved.

Should you encounter an unknown virus that cannot be disinfected, you can use the **FIND** option to restore the uninfected MBR from the rescue file that was created by either FIXDSKNT or the FIXDISK **RESCUE** option. This option allows you to access your valuable data files. Use of the **FIND** and other FIXDISK-related options is detailed below.

Repair

This option attempts a generic repair of the MBR. If this fails, it searches the hard drive for a rescue file. For example, at the command line type the following and press **Enter**:

```
FIXDISK REPAIR A:
```

Save

This option stores an image of the first track of the drive and the boot sector.

This is the preferred method to use if sending Command Software a suspected virus sample for analysis. Also, if you use NTFS, it is recommended that you save this information to a diskette as you can then use the Command AntiVirus DOS recovery utilities if necessary. For example, at the command line type the following and press **Enter**:

```
FIXDISK SAVE C:
```

The system prompts you to enter a network path and a file name. The file name should be in the 8.3 format so that the DOS version of Command AntiVirus can be used, if needed, to recover your data. The file name must also include the .DAT extension.

Undo

This option allows you to restore the boot area to the state it was in before you repaired it. It will ask for the name of the rescue file so have that information on hand. For example, at the command line, type the following and press **Enter**:

```
FIXDISK UNDO C:
```

Find

This option skips the generic repair and searches for the rescue file on the hard drive. This search is done on a track-by-track basis and may take some time. If you have already deleted the rescue file, but its contents have not yet been overwritten, this option recovers the information and restores your hard drive. For example, at the command line, type the following and press **Enter**:

```
FIXDISK FIND
```

Rescue

This option restores a rescue file. The **RESCUE** option is always with the **RESTORE** option.

Restore

The **RESTORE** option can be used if you have a specific, previously saved rescue file that you would like to use for boot record disinfection. For example, at the command line, type the following and press **Enter**:

```
FIXDISK RESCUE RESTORE
```

The system prompts you for the rescue file name to use for recovering the MBR and boot sector.

DISINFECTING A BOOT SECTOR VIRUS

There are two ways to safely disinfect a boot sector virus using FIXDISK.EXE. The easiest way is with a previously created Command AntiVirus rescue disk set. For more information on creating a rescue disk set, refer to the ***Installation*** chapter of this guide. A different method is used if you have just attempted to install Command AntiVirus and have detected a preexisting master boot record or boot sector virus.

Disinfecting with the Command AntiVirus Rescue Disk Set

The Command AntiVirus rescue disk process involves two phases. The first phase focuses on recovery by detecting and removing any executable, boot sector, and MBR-infecting viruses that inhibit or prevent system startup.

After successful recovery, the second phase focuses on scanning and disinfecting all remaining virus-infected files, for example, macro virus-infected files.

To assure a successful rescue, you **must** perform both phases.

NOTE: For NTFS systems, unless you can access an NTFS drive from within DOS, for example, by using third-party software, you will **not** be able to use the rescue disk set to scan files on an NTFS drive.

You can use **Rescue Disk 1** on NTFS systems at any time to repair damaged or infected boot sector information.

To perform Phase One, 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
   ```

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.
11. Proceed to **Phase Two**.

To perform Phase Two, follow these steps:

1. Restart your computer as normal.
2. Use Command AntiVirus to perform a scan of your local hard drives. This scan detects and disinfects any remaining virus-infected files on your computer.

After completing the **Phase Two** scan, you can return to computing as normal.

Disinfecting without a Startup Diskette

1. Turn off your computer.
2. Place a virus-free, write-protected bootable diskette (DOS Version 5.0 or higher) into drive A.
3. Turn on your computer to boot DOS.
4. Remove the bootable diskette from drive A.
5. Run F-PROT.EXE (this is the DOS version of Command AntiVirus) from the Command AntiVirus CD. You may be able to recover the MBR/boot sector without needing to reinstall Windows.
6. If F-PROT.EXE **cannot** recover the MBR/boot sector, run FIXDISK.EXE as described earlier in this chapter. It is also on the Command AntiVirus CD.

   If F-PROT.EXE or FIXDISK.EXE removed the infection, continue to **Step 7**.

   If F-PROT.EXE or FIXDISK.EXE do **not** remove the infection, reinstall the Windows® operating system. Perform an upgrade **not** a new installation. Then, continue to **Step 7**.

7. Install Command AntiVirus.
8. Perform a full scan of your hard drives.
9. Create a Command AntiVirus rescue disk set. For more information, refer to the ***Installation*** chapter of this guide.

NOTE: FIXDISK.EXE repairs only MBRs whose partition tables have **not** been modified by a virus. If a virus has modified the partition table and you have a FIXDISK-created rescue file, a successful repair can be made.

IF DISINFECTING FAILS

Should attempts to disinfect a boot sector virus fail, check the CMOS setup of the infected system.

NOTE: Many computers allow you to change their CMOS settings by pressing a specific key or by using a certain keystroke combination during startup. If your computer's startup sequence does not display which key or keystroke combination you can use, consult your owner's manual or your computer's manufacturer for specific information on how to access the CMOS settings.

Some boot sector virus variants try to protect themselves by modifying the computer's CMOS settings. For example, sometimes a virus will turn **off** the boot sector protection in CMOS, infect the boot sector and then turn the protection back on. Make sure that your computer's boot sector protection is turned **off**.

A second method that some viruses use to infect systems consists of changing the boot sequence so that the computer boots first from drive C instead of drive A. Thus, when you perform a cold boot, the virus loads first and then searches the floppy drive for a copy of DOS, appearing to boot properly. Make sure that the boot sequence in CMOS has drive A selected as the initial boot drive.

5

DOS RECOVERY

This chapter explains the Command AntiVirus (CSAV) menu and command-line options that can be used in the DOS environment. In an emergency, you can boot from a DOS system disk and use your Command AntiVirus rescue disk set with the options that are detailed in the following sections. You can also run a DOS-based Command AntiVirus scan from your hard drive.

Regardless of whether you start a DOS-based scan from your rescue disk set or from your computer's hard drive, the scan is started by running the file called **F-PROT.EXE**. After disinfecting any file and boot sector viruses, you can then restart your computer as normal, scan from your hard drive and disinfect any macro viruses that may exist on your system.

In addition to **F-PROT.EXE**, Command AntiVirus includes additional utilities. These utilities are used to clean damaged or virus-infected boot sectors. For more information, refer to the ***Boot Record Support*** chapter of this guide.

F-PROT.EXE can be run from DOS in both menu-driven and command-line modes. You can find a list of the command-line switches in **Command-Line Mode** located in this chapter. In **F-PROT.EXE Menu Options**, you can find the selections that are available from the Command AntiVirus for DOS menus.

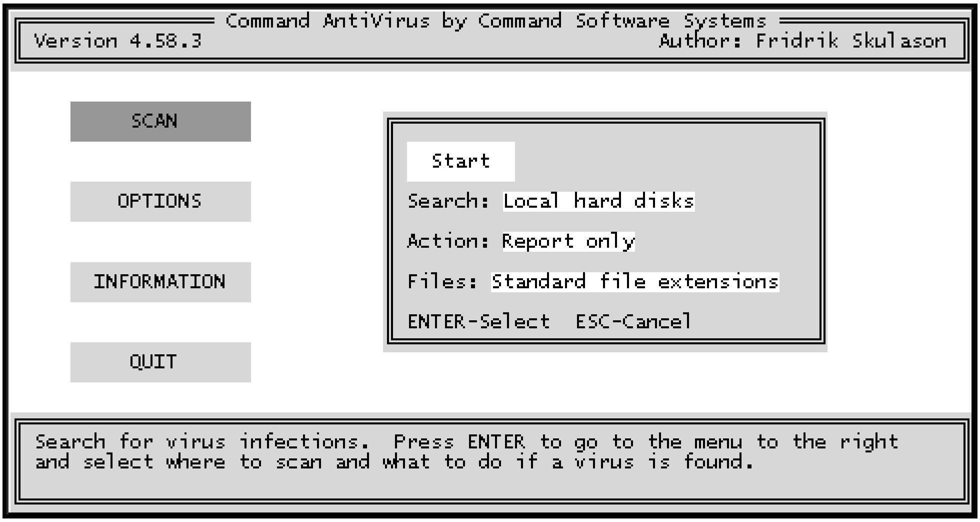
NOTE: For NTFS systems, unless you can access an NTFS drive from within DOS, for example, by using third party software, you will **not** be able to use the rescue disk set to scan files on an NTFS drive.

You can use **Rescue Disk 1** on NTFS systems at any time to repair damaged or infected boot sector information.

F-PROT.EXE MENU OPTIONS

The following directions will help you start a virus scan using the DOS-based menu. Be sure to change to the appropriate directory if you have not installed to the default **F-PROT** directory. At the DOS command line:

1. Type **CD \F-PROT**
2. Press **Enter**.
3. Type **F-PROT**
4. Press **Enter**. After **F-PROT.EXE** completes a scan for any viruses that may be in memory, the system displays the **Main** menu:



```
Command AntiVirus by Command Software Systems
Version 4.58.3                          Author: Fridrik Skulason

Search: Local hard disks
Action: Report only
Files: Standard file extensions

Search for virus infections.  Press ENTER to go to the menu to the right
and select where to scan and what to do if a virus is found.
```

Main Menu

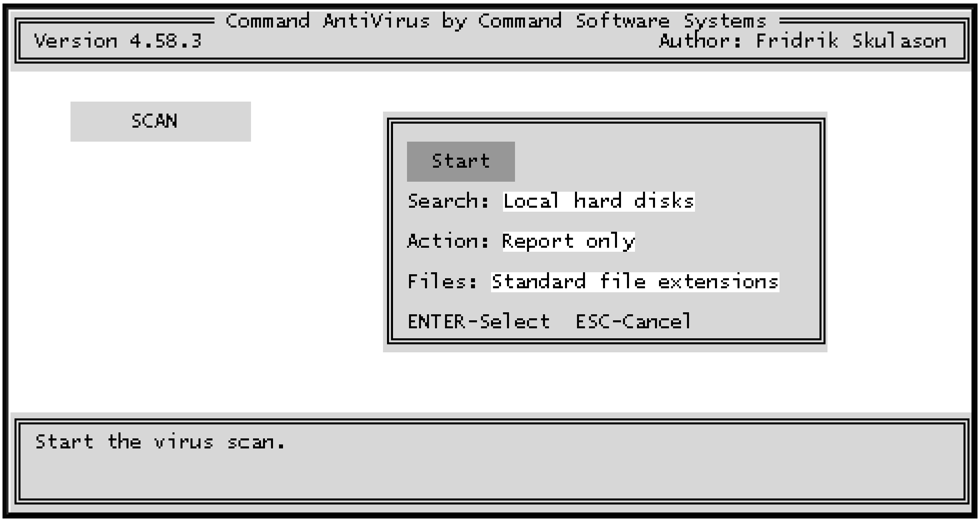
You can select an item from the menu by using the arrow keys to highlight the appropriate command and then pressing **Enter**.

NOTE: When an item is selected, a description of the item appears in an information box at the bottom of the screen. From any screen, you can go back to the previous screen by pressing the **ESC** key.

The following section describes these items in detail.

SCAN

When you select **Scan** from the **Main Menu,** the system displays the **Scan** menu:



Command AntiVirus by Command Software Systems

Version 4.58.3 Author: Fridrik Skulason

Search: Local hard disks

Action: Report only

Files: Standard file extensions

Start the virus scan.

Scan Menu

From this menu, you can select the type of drives the program scans for viruses. For example, the program can scan a local hard drive, diskette drive or network drives. You can also select the action to take when a virus is found and what type of files are to be scanned.

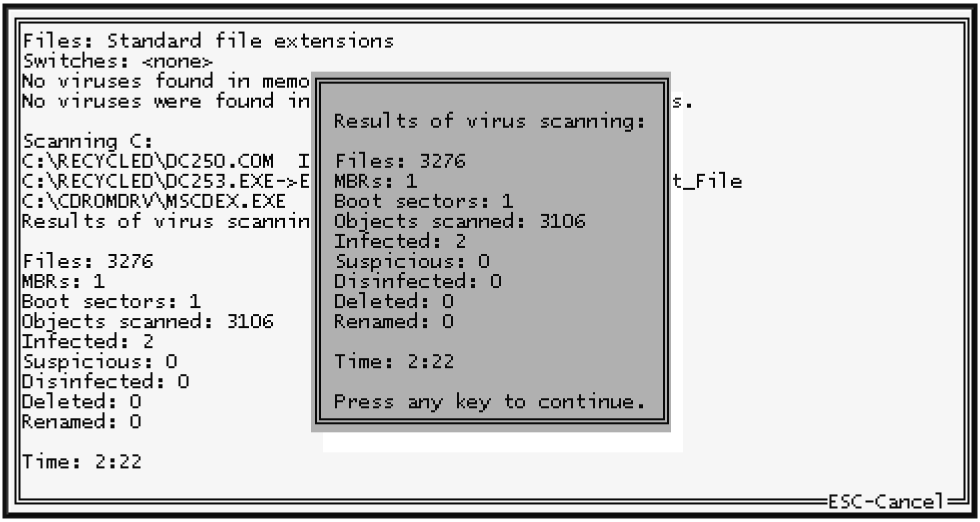
The following descriptions will help you decide which options to select.

Start

When you select this option and press **Enter**, the scan begins immediately.

NOTE: You can press **ESC** at anytime to stop a scan in progress.

When the scan is complete, the system displays the following results box. The system also displays a **Results of Virus Scanning** report. You can scroll through this report or send it to a printer or a disk file.



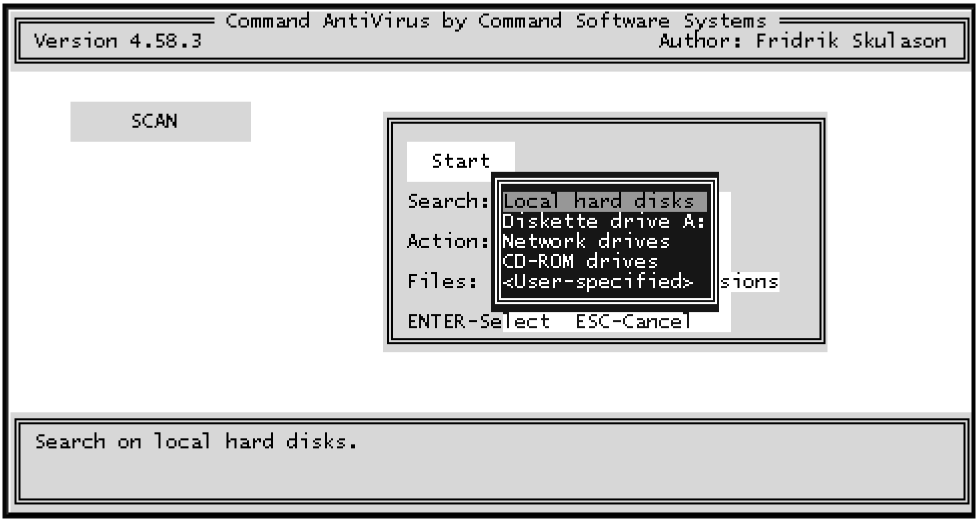
```
Files: Standard file extensions
Switches: <none>
No viruses found in memo
No viruses were found in                            s.

Scanning C:
C:\RECYCLED\DC250.COM  I
C:\RECYCLED\DC253.EXE->E                            t_File
C:\CDROMDRV\MSCDEX.EXE
Results of virus scannin

Files: 3276
MBRs: 1
Boot sectors: 1
Objects scanned: 3106
Infected: 2
Suspicious: 0
Disinfected: 0
Deleted: 0
Renamed: 0

Time: 2:22
```

```
Results of virus scanning:

Files: 3276
MBRs: 1
Boot sectors: 1
Objects scanned: 3106
Infected: 2
Suspicious: 0
Disinfected: 0
Deleted: 0
Renamed: 0

Time: 2:22

Press any key to continue.
```

Results of Virus Scanning

Search

When you select this option, the system displays the **Scan Search** menu:



```
Command AntiVirus by Command Software Systems
Version 4.58.3                          Author: Fridrik Skulason

   SCAN

                     Start
                     Search: Local hard disks
                             Diskette drive A:
                     Action: Network drives
                             CD-ROM drives
                     Files:  <User-specified> sions

                     ENTER-Select  ESC-Cancel

Search on local hard disks.
```

Scan Search Menu

From this menu, you can select which drives Command AntiVirus should scan for viruses. You can select only **one** of the following search options at a time:

Local Hard Disks

This option scans your local hard drives. By default, Command AntiVirus scans all logical and physical drives automatically.

Diskette Drive A:

This option scans floppy disks in drive A for viruses.

Network Drives

This option scans any network drives that are mapped to a drive letter.

CD-ROM Drives

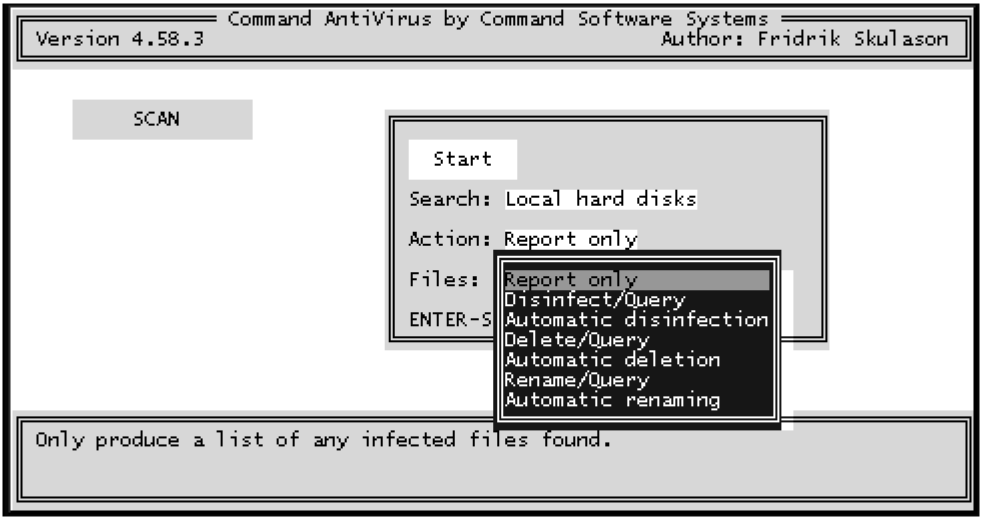
This option scans CDs.

User-Specified

This option allows you to specify a particular drive/path to scan. The **User-specified** option is particularly useful when you want to scan newly created directories after installing a new program.

Action

When you select this option, the system displays the **Scan Action** menu:



```
Command AntiVirus by Command Software Systems
Version 4.58.3                          Author: Fridrik Skulason

SCAN

Start
Search: Local hard disks
Action: Report only
Files:  Report only
        Disinfect/Query
ENTER-S Automatic disinfection
        Delete/Query
        Automatic deletion
        Rename/Query
        Automatic renaming

Only produce a list of any infected files found.
```

Scan Action Menu

NOTE: From the **Scan Action Menu**, you can select the type of action to take when a virus is found. The default is **Report Only**.

If you choose to disinfect a file when a virus is found, make sure that you can run Command AntiVirus after restarting the computer from a virus-free, write-protected system diskette. We recommend this scanning process because, if a virus remains active in memory, the virus may interfere with the disinfection process.

The following descriptions will help you decide which option to select:

Report Only

This option displays the scan results in a report at the end of the scan. The program takes no other action. You can scroll through this report or send it to a printer or a disk file.

Disinfect/Query

This option prompts you before disinfecting a file. Command AntiVirus can disinfect most non-overwriting viruses.

Automatic Disinfection

This option disinfects files automatically when Command AntiVirus finds a virus. Use **Automatic Disinfection** with caution as no prompt appears prior to disinfection.

Also, some viruses cannot be disinfected. In these cases, the infected files are deleted automatically. No prompt appears prior to deletion.

Delete / Query

This option prompts you before deleting an infected file.

Automatic Deletion

This option deletes infected files automatically. We do not recommend **Automatic Deletion** as some viruses encrypt portions of the hard disk. When the program removes the virus, the encrypted portions are lost.

If you think that you have a virus that uses encryption, contact your local support representative. There are at least two types of encryption and two methods of disinfection. Your support representative will be able to help you use the proper method without any loss of data.

Before selecting this option, be sure that you have a virus-free backup for all installed software and files.

Rename/Query

NOTE: This option renames infected files so that their extensions begin with a V. For example, if a file named MYDOC.EXE contains a virus, the program renames the file to MYDOC.VXE. As you cannot run files with a .VXE extension, these files are **not** a threat to your system.

Before Command AntiVirus renames the suspected file, the program asks you if you want the file extension changed.

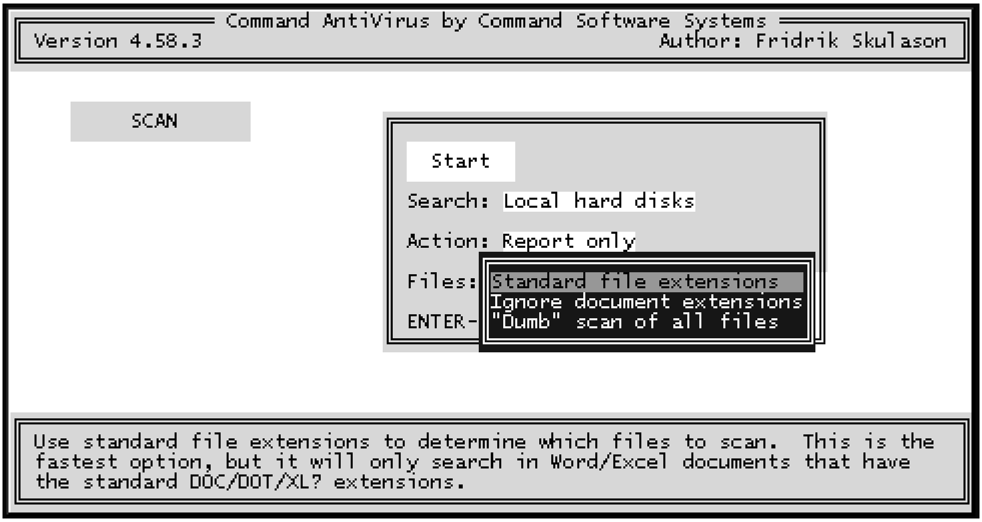
Use this option if you want study the infected file or compare it to a virus-free backup copy.

Automatic Renaming

This option is similar to **Rename/Query**, but the program does not prompt you prior to renaming the file's extension.

Files

When you select this option, the system displays the **Scan Files** menu:



```
Version 4.58.3    Command AntiVirus by Command Software Systems
                                          Author: Fridrik Skulason

    SCAN
                         Start

                         Search: Local hard disks

                         Action: Report only

                         Files: Standard file extensions
                                Ignore document extensions
                         ENTER- "Dumb" scan of all files

Use standard file extensions to determine which files to scan.  This is the
fastest option, but it will only search in Word/Excel documents that have
the standard DOC/DOT/XL? extensions.
```

Scan Files Menu

The **Files** option allows you to select which file types to scan. The following descriptions will help you to decide which options to select:

Standard File Extensions

These are the file types that are normally targeted by viruses for infection. To provide the most up-to-date anti-virus protection, the default extensions that are scanned may change from one version of Command AntiVirus to another.

Ignore Document Extensions

This option scans document files even if you use an extension other than .DOC or .DOT.

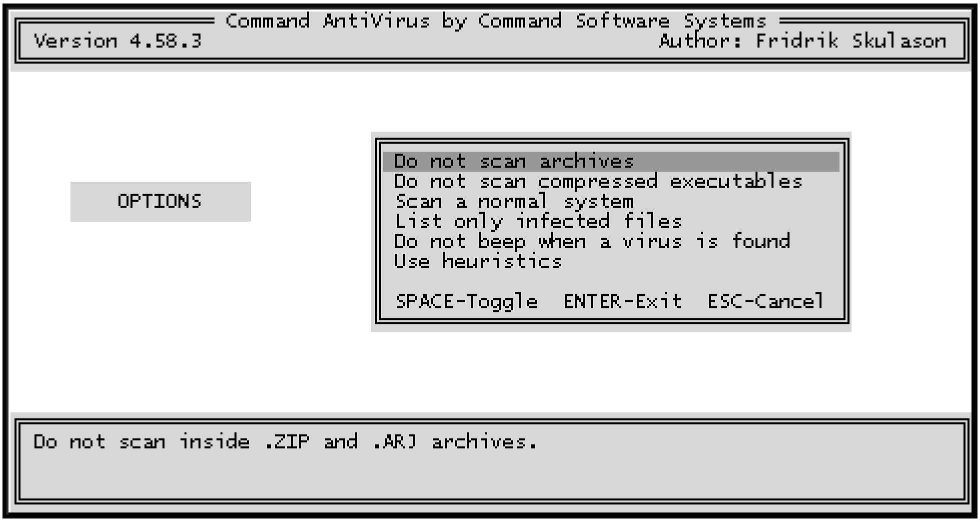
“Dumb” Scan of All Files

This option scans every file. We do not recommend this option for inexperienced users as scanning all files on a disk could produce a false indication of a virus. Use this option only if one of the following conditions exists:

- A virus has been found on the computer.
- You want to make sure a virus is not hiding in some obscure place.
- You are concerned that a misnamed file may contain a virus that could later be activated by renaming and running the file.

OPTIONS

When you select this option, the system displays the **Options** menu:



```
Command AntiVirus by Command Software Systems
Version 4.58.3                                  Author: Fridrik Skulason

OPTIONS         Do not scan archives
                Do not scan compressed executables
                Scan a normal system
                List only infected files
                Do not beep when a virus is found
                Use heuristics

                SPACE-Toggle  ENTER-Exit  ESC-Cancel

Do not scan inside .ZIP and .ARJ archives.
```

Options Menu

Each option is either **on** or **off**. Selecting the option and pressing the spacebar changes the option between **on** and **off**. For example, if you select the **Do not scan archives** option and press the spacebar, the option setting changes to **Scan Archives**.

The following descriptions will help you decide which option to select.

Do Not Scan Archives

This option does not scan inside archives.

Do Not Scan Compressed Executables

This option does **not** scan compressed executable files that may have been infected before compression.

Selecting this option may cause the scanner miss some virus “droppers”.

Scan a Normal System

This option scans only for viruses and other “malware” that may be found on a normal system. It does **not** scan for infected boot sector image files or other similar material that is normally found only in virus collections.

List Only Infected Files

This option lists in the report file only those files that are found to be infected or are considered suspicious.

Do Not Beep When a Virus Is Found

This option allows you to select whether or not your computer will emit a beep when a virus is found.

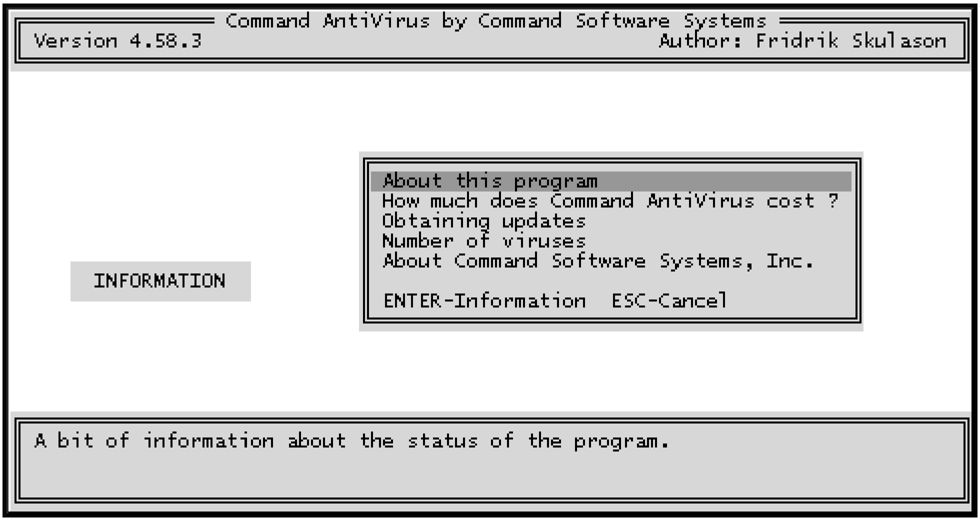
Use Heuristics

This option allows you to select the heuristics scanning method.

Heuristic scanning does not rely on specific virus signatures. It uses behavioral patterns as well as a set of rules to identify the type of code that viruses use. This is not a recommended option for inexperienced users as it may return occasional false positives.

INFORMATION

This menu item provides information about Command AntiVirus. When you select **Information** from the Main Menu, the system displays the **Information** menu:



```
Command AntiVirus by Command Software Systems
Version 4.58.3                                      Author: Fridrik Skulason

                      About this program
                      How much does Command AntiVirus cost ?
                      Obtaining updates
                      Number of viruses
                      About Command Software Systems, Inc.
  INFORMATION
                      ENTER-Information  ESC-Cancel

A bit of information about the status of the program.
```

Information Menu

The following descriptions will help you decide which option to select.

About This Program

This option provides information about the status of the program.

How Much Does Command AntiVirus Cost?

This option provides addresses, telephone numbers and other information on how you can obtain pricing information on Command AntiVirus.

Obtaining Updates

This option provides addresses, telephone numbers and other information about organizations that you can contact for updating your copy of Command AntiVirus.

Number of Viruses

This option provides information on approximately how many viruses Command AntiVirus detects.

About Command Software Systems, Inc.

This option provides information about the author and publisher of the program.

QUIT

This menu item allows you to exit F-PROT.EXE. When you select **Quit**, the system asks if you want to save the changes that you may have made to F-PROT.EXE's settings. Type Y or N. The program stores the setup information in a file named SETUP.F2.

COMMAND-LINE MODE

Instead of using the DOS-based graphical menu, you can also run the program in command-line mode. To use the program in command-line mode, you need to run F-PROT.EXE with at least one of the command-line switches shown in the following table. The order of the switches is not critical.

Table 5-1: F-PROT.EXE Command-line Switches

Switch	Description
/APPEND	Appends a new report to an existing one. Use this with the /REPORT switch.
/ARCHIVE	Scans inside archives.
/AUTO	Use with /DELETE or /DISINF switch so that Command AntiVirus will not prompt you before deleting or disinfecting a file. When used without /AUTO, /DELETE and /DISINF prompt you before taking any action.
/BEEP	Generates a beep when a virus is found.
/COLLECT	Scans for a virus collection.
/DELETE	Deletes all infected files. We do not recommend using this switch as some viruses encrypt portions of the drive.
/DISINF	Disinfects whenever possible. This option deletes some overwriting and first-generation virus samples. A first-generation virus is the “starter” program that begins the infection process. Encountering a first generation virus is very rare. This option will never delete a file that CSAV can disinfect.
/DUMB	Scans **all** files. **Caution**: We do **not** recommend this option for inexperienced users as scanning all files on a disk could produce a false indication of a virus infection.
/FREEZE	Halts the computer when the program finds a virus.
/HARD	Scans all the physical hard drives in the system.
/HELP or /?	Displays a list of available options.

Table 5-1: F-PROT.EXE Command-line Switches

Switch	Description
/INTER	Forces interactive mode.
/LIST	Produces a list of all files checked, not just infected files.
/LOADDEF	Loads the definition files into memory. This allows you to perform a complete scan during recovery to detect and disinfect any virus-infected files. Note: Use of this switch increases your memory requirements.
/NOBOOT	Does **not** scan for MBR and boot sector viruses.
/NOBREAK	Does **not** allow users to end a scan with the **ESC** key. See **Restricting Users** located in the ***Network Administration*** chapter.
/NOFILE	Does **not** scan for file viruses.
/NOFLOPPY	This switch is for use on a system without floppy drives.
/NOHEUR	Disables heuristics.
/NOMEM	Does **not** scan memory for viruses.
/NOSUB	Does **not** scan subdirectories.
/PACKED	Unpacks compressed executables.
/PAGE	Pauses after every screen while displaying a report.
/REMOVEALL	Removes all macros from all documents.
/REMOVENEW	Removes new variants of macro viruses by removing all macros from infected documents.
/RENAME	Renames infected COM/EXE files to VOM/VXE. You can use this switch with /AUTO.
/REPORT=	Sends the output to the file you specify to the right of the equals (=) sign.
/SAFEREMOVE	Removes all macros from documents if a known virus is detected.
/SILENT	Generates **no** screen output at all. This is useful when running F-PROT.EXE from a batch file where you will check for return codes.

Table 5-1: F-PROT.EXE Command-line Switches

Switch	Description
/TODAY	The date of the last scan is stored in the F-PROT.DAT file. If the next scan finds the same date, Command AntiVirus will not repeat the scan.
/TYPE	Ignores extensions of Microsoft® Word and Excel files.
/VIRLIST	Lists the known viruses.
/VIRNO	Counts the known viruses.
/WRAP	Wraps text so the report fits in 78 columns.

The following example shows you how to run Command AntiVirus from the command-line. As the main reason you would be running the DOS version of Command AntiVirus is concern over a virus, we suggest that you run the scan from your floppy drive.

After starting your computer from a DOS system disk, remove the disk from the floppy drive. Then, insert the **CSAV Rescue Disk 1** into the floppy drive. Type the following at the A prompt and press **Enter**.

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

When you run **F-PROT.EXE** with the **/HARD** switch, it scans the boot records and executable files on all local, hard drives. The **/DISINF** switch tells **F-PROT.EXE** to identify a virus and then asks if you want to disinfect it. The **/LOADDEF** switch loads the definition files into memory so that you can complete the scan.

NOTE: After starting your computer from a DOS system disk and running the command-line version of **F-PROT.EXE** from the rescue disk set, remove any diskettes that are in your floppy drives and restart your computer as normal. Then, run Command AntiVirus from you hard disk. This hard disk-initiated scan disinfects any macro viruses that may remain on your system.

F-PROT.EXE RETURN CODES

F-PROT.EXE returns the following codes that you can check with the **ERRORLEVEL** command from a batch file. Use this command in your **AUTOEXEC.BAT** file to warn you if Command AntiVirus finds a problem.

For example, if the program produces the numeral 2 as a return code, you could notify the user that Command AntiVirus failed its self-test. You could then request that the user either notify a supervisor or take corrective action.

Table 5-2: F-PROT.EXE Return Codes

Return Codes	Descriptions
0	Nothing found, nothing done.
1	Unrecoverable error. This is usually the result of a missing system file.
2	Self-test failed or companion found.
3	At least one virus-infected object was found.
4	A virus is active in the system.
5	Abnormal termination (unfinished scan).
6	At least one virus was removed.
7	Unable to allocate sufficient memory.
8	Something suspicious was found but it was not a recognized virus.

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.

On computers running Windows® 2000, you can use Group Policy to deploy Command AntiVirus for Windows NT/2000 to individual computers from a central location on a network.

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 the **Automatic Update** section found later in this chapter.

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 protection against new viruses, we update Command AntiVirus frequently. You can download interim releases of the product from our web and FTP sites. You can also download the latest virus definition files. To protect your systems, be sure to keep your copy of Command AntiVirus up-to-date.

For more information on how to update Command AntiVirus, refer to **Definition Files Update Button** and **Automatic Update**.

In Command AntiVirus for Windows NT/2000, also refer to **Deploying Command AntiVirus through Group Policy**.

In addition to providing instructions on 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 TO A SOFTWARE DISTRIBUTION POINT (SDP)

We recommend that you perform an administrative installation of Command AntiVirus for Windows NT/2000 to your software distribution point (SDP). This allows you to easily apply and distribute future patches such as updates to our virus definition files.

You can perform the administrative installation for as many SDPs as needed. If you install Command AntiVirus features to run from the server or to be installed when the feature is first accessed, multiple SDPs ensure that there is always access to an available network server. You can then list these SDPs when you customize your installation settings using the Command AntiVirus Custom Installation Wizard.

To perform an administrative installation, at the command line, type the following and press **Enter**.

```
msiexec /a csav.msi
```

CUSTOMIZING YOUR SCAN TASKS

Command AntiVirus for Windows NT/2000 comes with several preconfigured scan tasks that are available immediately after you install the product. These scan tasks include the most commonly needed tasks such as:

- Scan Drive A
- Scan Drive B
- Scan Hard Drives
- Scan CD-ROM Drives
- Scan Network Drives

By default, all of these tasks are set to **Report only** if a virus is found.

After you have performed an administrative installation of Command AntiVirus for Windows NT/2000 to your SDPs, you can replace these default scan tasks with your own set of tasks prior to deployment. For more information on creating or customizing scan tasks, refer to **Using the Task Menu** in the ***Using Command AntiVirus*** chapter.

To replace the default Command AntiVirus scan tasks, follow these steps:

1. Go to your Software Distribution Point (SDP).
2. Search for the **WIN2000W\Installation Tools\Tasks** folder.

Search the CD for the **WIN2000S\Installation Tools\Tasks** folder.

3. Open that folder.
4. Replace the existing scan task files with your customized files.

NOTE: Make sure that you repeat these steps for each of your SDPs.

CUSTOMIZING YOUR COMMAND ANTIVIRUS UPDATES INFORMATION

Command AntiVirus for Windows NT/2000 comes with a preconfigured CSSFTP.INI file. This file contains information that is used in the Command AntiVirus download and scheduled update processes. The information includes FTP sites, **staging directory** location, **automatic update directory** location, and the time of scheduled downloads.

After you have performed an administrative installation of Command AntiVirus for Windows NT/2000 to your SDPs, you can edit the CSSFTP.INI file or replace it with your own customized file prior to deployment.

To customize or replace the default Command AntiVirus CSSFTP.INI file, follow these steps:

1. Go to your Software Distribution Point (SDP).
2. Search for the **WIN2000W\Installation Tools\CssFtp** folder.

Search the CD for the **WIN2000S\Installation Tools\CssFtp** folder.

3. Open that folder.
4. Using Notepad or any text editor, make changes to the default CSSFTP.INI file and save the file, or replace the default file with your customized file.

NOTE: Make sure that you repeat these steps for each of your SDPs.

CUSTOMIZING YOUR INSTALLATION SETTINGS

The Command AntiVirus Custom Installation Wizard allows you to customize the installation features and settings before you install Command AntiVirus over the network onto multiple computers.

The wizard uses the Command AntiVirus Windows installer package (MSI file) to create a custom Windows installer transform (MST file). This file contains the installation features and settings that you select and is used with the MSI file during deployment to customize your installation over the network. You can use the wizard to create a new MST file or to modify an existing file.

NOTE: No changes are made to the Command AntiVirus MSI file.

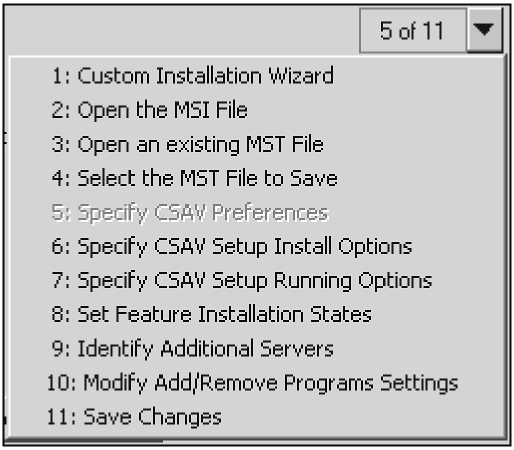
Using the Command AntiVirus Custom Installation Wizard, you can:

- **Specify CSAV Preferences** – Allows you to modify the default installation settings for the items on the Command AntiVirus **Preferences** menu. For more information, refer to **Using the Preferences Menu** in the ***Using Command AntiVirus*** chapter.
- **Specify CSAV Installation Options** – Allows you to prevent or allow the creation of the rescue disk set during installation. You can also change the default port locations for the communication subsystem.
- **Specify CSAV Application Options** – Allows you to prevent or allow access to certain features. You can also set the time that automatic updates take place.
- **Set Feature Installation States** – Allows you to select the features that you want to install and how they will be installed. You can also select whether the feature is displayed or hidden during the installation process and when the user is adding or removing features after CSAV is installed.
- **Identify Additional Servers** – Allows you to specify additional network servers that have a copy of the installation folder tree. If you install features to run from the server or to be installed when the feature is first accessed, this option ensures that there is always access to an available network server.

- **Modify Add/Remove Programs Settings** – Allows you to modify the information that is displayed in the Windows **Support Info** dialog box for Command AntiVirus. You can access this information through the Windows **Add/Remove Programs** dialog box in the Control Panel by selecting Command AntiVirus and clicking support information.

The wizard is easy to use. Just make your selections and click **Next** to continue. Here are just a few points to remember.

- To go back to the previous dialog box, click **Back**.
- To exit the wizard during the process, click **Cancel**.
- To save your changes to the MST file, click **Finish**.
- To exit the wizard after you have completed the process, click **Exit**.
- To go to any page in the wizard, click the down arrow to the right of the page number in the upper-right corner of the dialog box. The system displays the following drop-down list box containing the wizard page names and numbers. Just click the page that you want. This option is available starting with **Page 5**.


5 of 11
1: Custom Installation Wizard
2: Open the MSI File
3: Open an existing MST File
4: Select the MST File to Save
5: Specify CSAV Preferences
6: Specify CSAV Setup Install Options
7: Specify CSAV Setup Running Options
8: Set Feature Installation States
9: Identify Additional Servers
10: Modify Add/Remove Programs Settings
11: Save Changes

Wizard Page Number Box

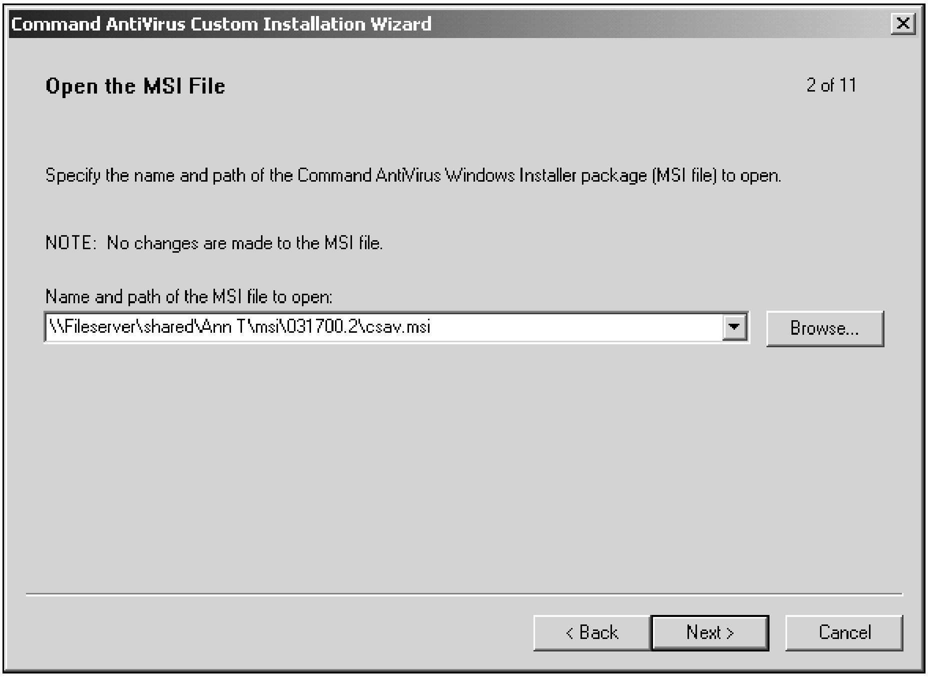
To start the wizard and create or modify an MST file, follow these steps:

1. Insert the CD-ROM.
2. Click the **Start** button on the Windows task bar.
3. Click **Run**.
4. Click **Browse** to search the CD for the **WIN2000W\Installation Tools\Wizard** folder.

SERVER

Click **Browse** to search the CD for the **WIN2000S\Installation Tools\Wizard** folder.

5. Open that folder.
6. Double-click **CSAVWIZ.EXE**. The system returns to the **Run** dialog box.
7. Click **OK**. The system displays the **Welcome** dialog box.
8. Click **Next**. The system displays the **Open the MSI File** dialog box:



Command AntiVirus Custom Installation Wizard

Open the MSI File

2 of 11

Specify the name and path of the Command AntiVirus Windows Installer package (MSI file) to open.

NOTE: No changes are made to the MSI file.

Name and path of the MSI file to open:

\\Fileserver\shared\Ann T\msi\031700.2\csav.msi

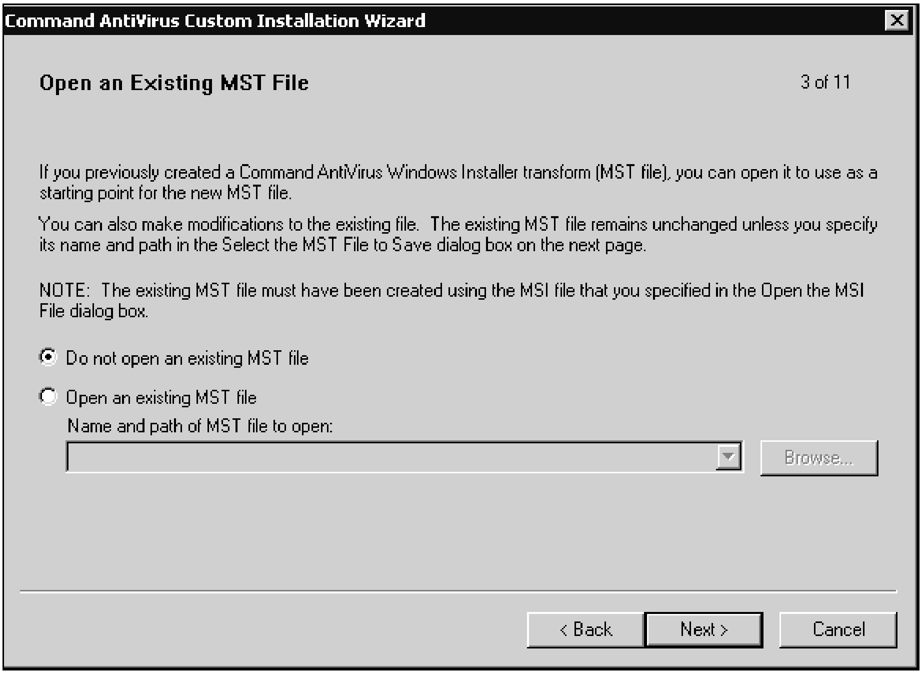
Open the MSI File Dialog Box

9. In the **Name and path of the MSI file to open** text box, type the path and name of the Command AntiVirus MSI file that you want to customize, for example:

```
S:\AnnT\csav2000\csav.msi
```

NOTE: You can also use the **Browse** button to search for the file. No changes are made to the MSI file.

10. Click **Next**. The system displays the **Open an Existing MST File** dialog box:



Command AntiVirus Custom Installation Wizard

Open an Existing MST File

3 of 11

If you previously created a Command AntiVirus Windows Installer transform (MST file), you can open it to use as a starting point for the new MST file.

You can also make modifications to the existing file. The existing MST file remains unchanged unless you specify its name and path in the Select the MST File to Save dialog box on the next page.

NOTE: The existing MST file must have been created using the MSI file that you specified in the Open the MSI File dialog box.

● Do not open an existing MST file

○ Open an existing MST file

Name and path of MST file to open:

Open an Existing MST File Dialog Box

11. If you have **not** previously created a Command AntiVirus MST file, select **Do not open an existing MST** file.

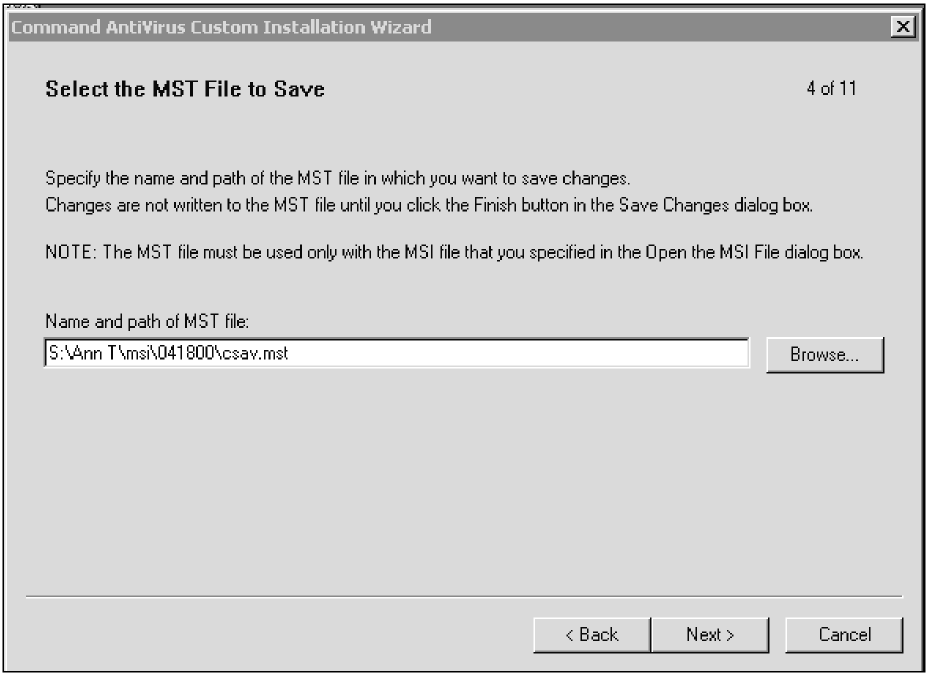
    If you have previously created a Command AntiVirus MST file, you can open the existing MST file to use as a starting point for a new file. You can also make changes to the existing file.

    Select **Open an existing MST file**. Then, type the path and name of the MST file in the **Name and path of MST file to open** text box.

NOTE: You can also use the **Browse** button or select a previously opened MST file from the drop-down list box.

The existing Command AntiVirus MST file must have been created using the Command AntiVirus MSI file that you specified in the **Open the MSI File** dialog box. The MST file remains unchanged unless you specify its path and name in the **Select the MST File to Save** dialog on the next page.

12. Click **Next**. The system displays the **Select the MST File to Save** dialog box:



Select the MST File to Save

4 of 11

Specify the name and path of the MST file in which you want to save changes.
Changes are not written to the MST file until you click the Finish button in the Save Changes dialog box.

NOTE: The MST file must be used only with the MSI file that you specified in the Open the MSI File dialog box.

Name and path of MST file: S:\Ann T\msi\041800\csav.mst

Select the MST File to Save Dialog Box

13. In the **Name and path of MST file** text box, type the path and name of the Command AntiVirus MST file in which you want to save the changes.

    For example, if you are creating a new MST file, type in a path and a file name including the .mst extension.

If you are updating an existing MST file, type in the path and the file name of the Command AntiVirus MST file that you previously opened in the **Open the MST file** dialog box. The system displays a dialog box asking you to confirm that you want to overwrite the existing file. Click **OK** to confirm.

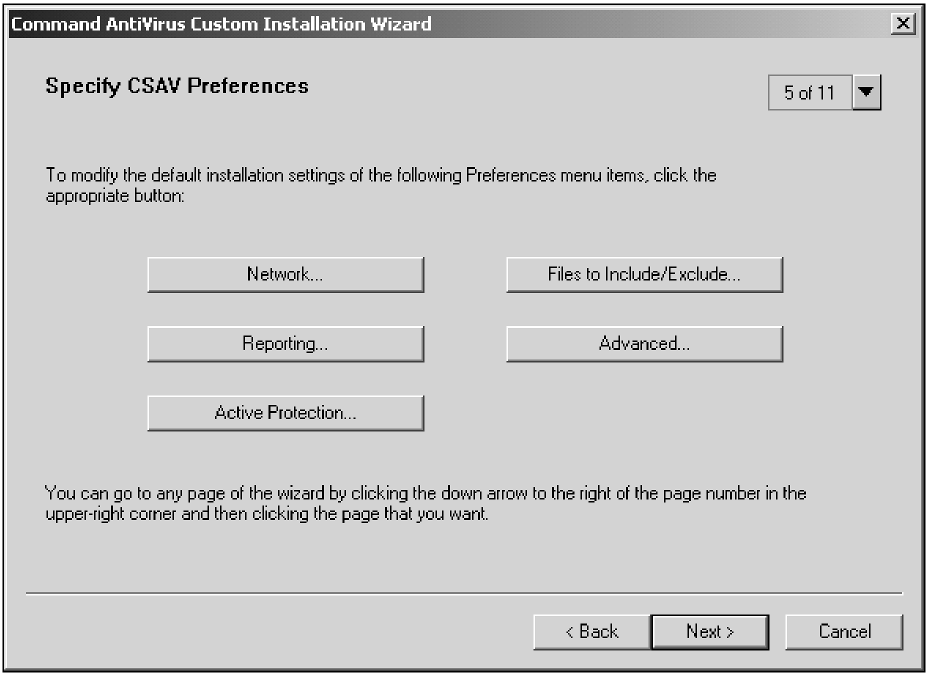
The changes are not written to the MST file until you are in the **Save Changes** dialog box.

NOTE: You can also use the **Browse** button to search for a file and/or path.

The Command AntiVirus MST file must be used only with the Command AntiVirus MSI file that you previously specified in the **Open the MSI File** dialog box.

For deployment, we recommend that the Command AntiVirus MST file be in the same folder as the Command AntiVirus MSI file.

14. Click **Next.** The system displays the **Specify CSAV Preferences** dialog box:



Command AntiVirus Custom Installation Wizard

Specify CSAV Preferences

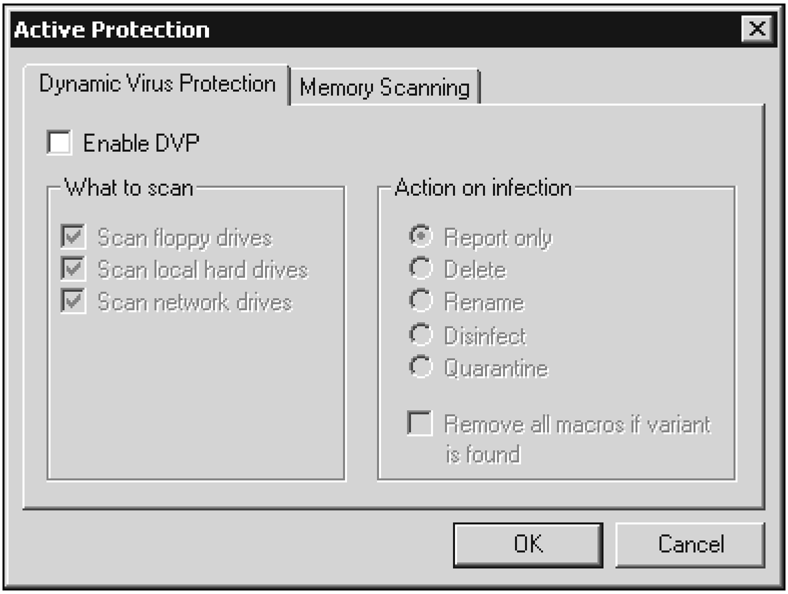
To modify the default installation settings of the following Preferences menu items, click the appropriate button:

You can go to any page of the wizard by clicking the down arrow to the right of the page number in the upper-right corner and then clicking the page that you want.

Specify CSAV Preferences Dialog Box

NOTE: Starting with this page, you can go to any page in the wizard by clicking the down arrow to the right of the page number in the upper-right corner and then clicking the page that you want.

15. Click the button of the item that you want to modify, for example, **Active Protection**. The system displays the appropriate dialog box:



Active Protection

Dynamic Virus Protection | Memory Scanning

□ Enable DVP

What to scan

☑ Scan floppy drives
☑ Scan local hard drives
☑ Scan network drives

Action on infection

● Report only
○ Delete
○ Rename
○ Disinfect
○ Quarantine

□ Remove all macros if variant is found

OK | Cancel

Active Protection Dialog Box

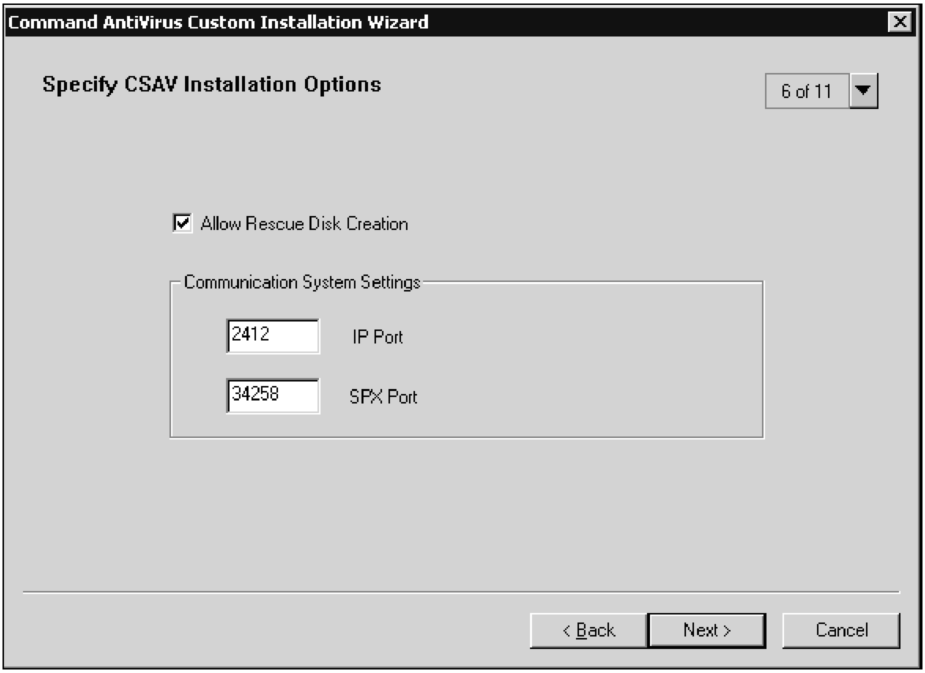
NETWORK ADMINISTRATION

NOTE: For more information on the Command AntiVirus **Preferences** menu items, refer to **Using the Preferences Menu** in the ***Using Command AntiVirus*** chapter.

16. Select the options that you want and click **OK**.

    Repeat **Steps 15** and **16** for each item that you want to modify.

17. When you have completed your changes, click **Next.** The system displays the **Specify CSAV Installation Options** dialog box:


Command AntiVirus Custom Installation Wizard

Specify CSAV Installation Options

6 of 11

☑ Allow Rescue Disk Creation

Communication System Settings

2412 IP Port

34258 SPX Port

Specify CSAV Installation Options Dialog Box

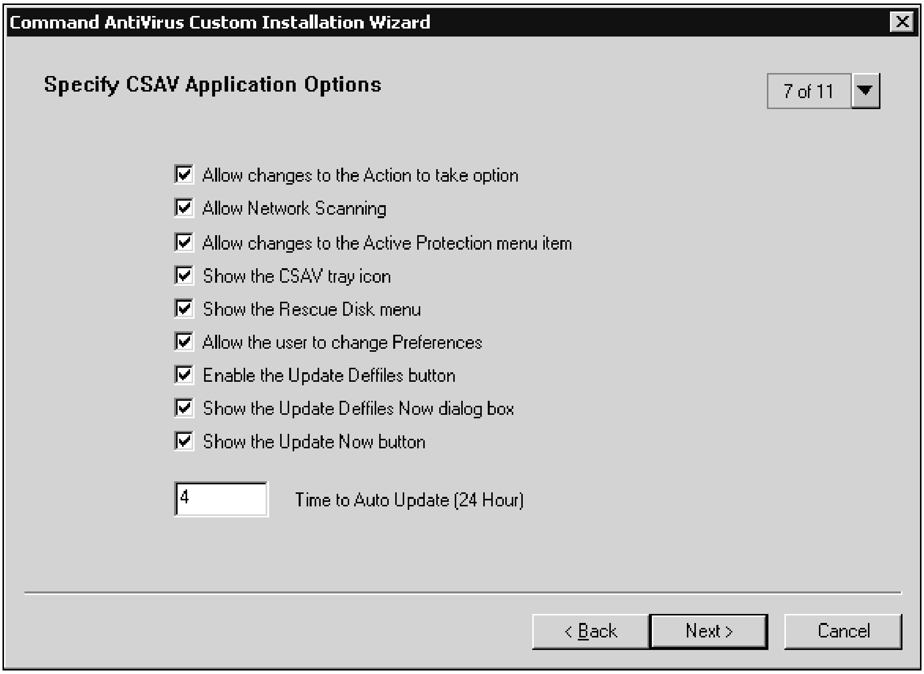
18. Select or clear the following check box. This option is selected by default.

    - **Allow Rescue Disk Creation** – Allows users to create a rescue disk set during the installation.

NOTE: To create a rescue disk set, the user **must** be a member of the local Administrators group.

19. The **IP Port** and the **SPX Port** text boxes contain the default port locations for the communication subsystem that is used by CSS Central for managing Command AntiVirus. If it is necessary, you can change these locations by typing a new number in each of the text boxes.

20. Click **Next**. The system displays the **Specify CSAV Application Options** dialog box:



Command AntiVirus Custom Installation Wizard

Specify CSAV Application Options

☑ Allow changes to the Action to take option
☑ Allow Network Scanning
☑ Allow changes to the Active Protection menu item
☑ Show the CSAV tray icon
☑ Show the Rescue Disk menu
☑ Allow the user to change Preferences
☑ Enable the Update Deffiles button
☑ Show the Update Deffiles Now dialog box
☑ Show the Update Now button

4 Time to Auto Update (24 Hour)

Specify CSAV Application Options Dialog Box

21. Select or clear any of the following options. All of these options are selected by default.

- **Allow changes to the Action to take option** – Allows users to modify the default setting for the **Action to take** option in the task's **Properties** dialog box. When you clear this check box, the **Action to take** option is dimmed. For more information, refer to **Scanning Properties** in the ***Using Command AntiVirus*** chapter.

- **Allow Network Scanning** – Allows users to scan network drives. When you clear this check box, the **Scan Network Drives** task in the **Command AntiVirus Main** dialog box is **not** shown. For more information, refer to **Task List** in the ***Using Command AntiVirus*** chapter.

- **Allow changes to the Active Protection menu item** – Allows users to modify the default settings for the **Active Protection** item on the Command AntiVirus **Preferences** menu. When you clear this check box, the **Active Protection** item is **not** shown. For more information, refer to **Active Protection** in the ***Using Command AntiVirus*** chapter.

- **Show the CSAV tray icon** – Displays the yellow **C** icon in the system tray at the bottom of your screen. This icon allows you to open Command AntiVirus or the **F-Agent Shortcut** menu. When you clear this check box, the yellow **C** icon is **not** shown. For more information, refer to **Other Ways to Access Command AntiVirus** in the ***Using Command AntiVirus*** chapter.

- **Show the Rescue Disk menu** – Displays the **Rescue Disk** menu option on the Command AntiVirus menu bar. When you clear this check box, the **Rescue Disk** menu option is **not** shown. For more information, refer to **Using the Rescue Disks Menu** in the ***Using Command AntiVirus*** chapter.

NOTE: To create a rescue disk set, the user **must** be a member of the local Administrators group.

- **Allow the user to change Preferences** – Allows users to modify the default settings for the items on the Command AntiVirus **Preferences** menu. When you clear this check box, the dialog boxes for the **Preferences** menu items say “locked” and the **OK** button on each dialog box is dimmed. For more information, refer to **Using the Preferences Menu** in the ***Using Command AntiVirus*** chapter.

- **Enable the Update Deffiles button** – Displays the **Update Deffiles** button in the **Command AntiVirus Main** dialog box. When you clear this check box, the **Update Deffiles** button is dimmed. For more information, refer to **Definition Files Update Button** located later in this chapter.

NOTE: If you are managing software installation through Group Policy and/or you have not configured the users to install with elevated privileges, we recommend that you clear this check box.

- **Show the Update Deffiles Now dialog box** – Displays the **Update Deffiles Now** dialog box. When you clear this check box, the **Update Deffiles Now** tab of the **Preferences/Advanced** dialog box is **not** shown. For more information, refer to **Definition Files Update Button** located later in this chapter.

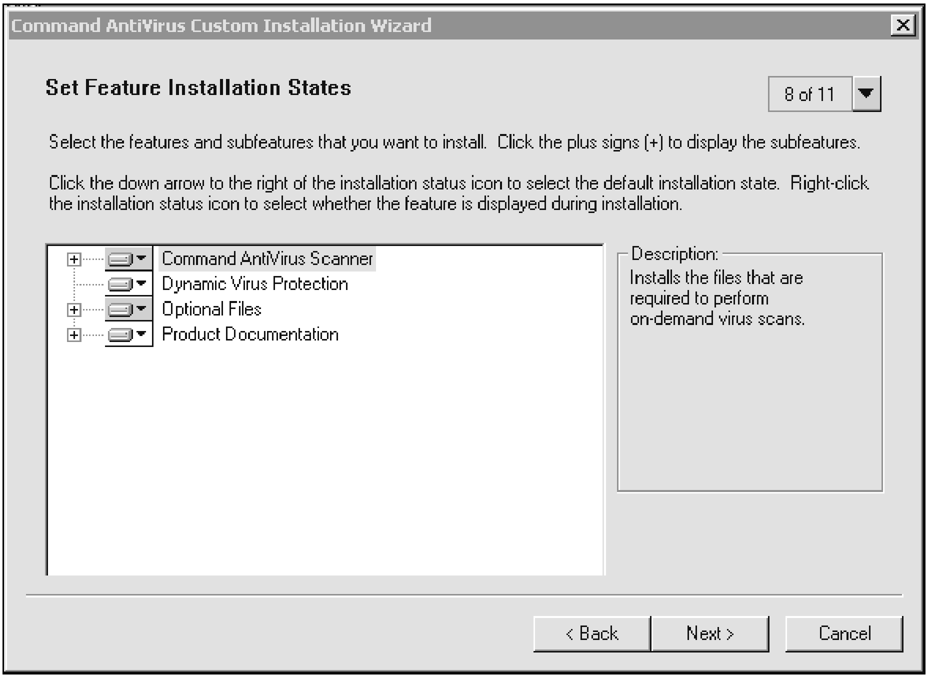
NOTE: If you are managing software installation through Group Policy and/or you have not configured the users to install with elevated privileges, we recommend that you clear this check box.

- **Show the Update Now button** – Displays the **Update Now** button in the **Automatic Update** tab of the **Preferences/Advanced** dialog box. When you clear this check box, the **Update Now** button is **not** shown. For more information, refer to **Automatic Update** located later in this chapter.

NOTE: If you are managing software installation through Group Policy and/or you have not configured the users to install with elevated privileges, we recommend that you clear this check box.

22. In the **Time to Auto Update** text box, type the hour (in 24-hour format) that automatic updates should take place. Specify the time in only hours using integers of **0** through **23**. For example, to start the update at 1:00 p.m. type *13*. The default time is set to *4* which is equal to 4:00 a.m.

23. Click **Next**. The system displays the **Set Feature Installation States** dialog box:



Command AntiVirus Custom Installation Wizard

Set Feature Installation States

Select the features and subfeatures that you want to install. Click the plus signs (+) to display the subfeatures.

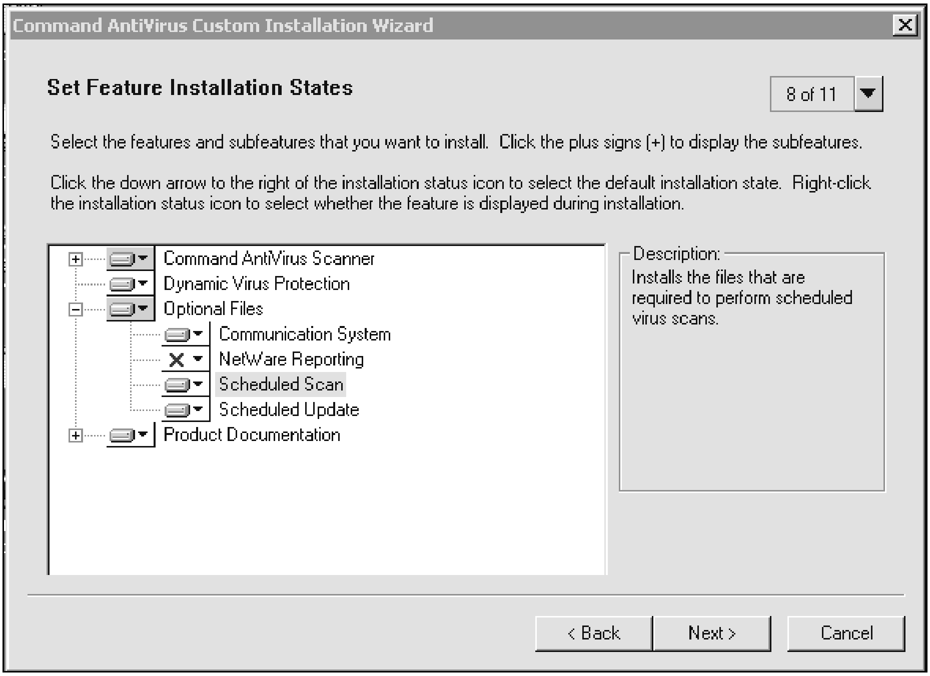
Click the down arrow to the right of the installation status icon to select the default installation state. Right-click the installation status icon to select whether the feature is displayed during installation.

- Command AntiVirus Scanner
- Dynamic Virus Protection
- Optional Files
- Product Documentation

Description:
Installs the files that are required to perform on-demand virus scans.

Set Feature Installation States Dialog Box

24. Select the features and subfeatures that you want to install. Click the plus signs (+) to display the subfeatures. You can view the description of each feature and subfeature by clicking its name.



Command AntiVirus Custom Installation Wizard

Set Feature Installation States

8 of 11

Select the features and subfeatures that you want to install. Click the plus signs (+) to display the subfeatures.

Click the down arrow to the right of the installation status icon to select the default installation state. Right-click the installation status icon to select whether the feature is displayed during installation.

- Command AntiVirus Scanner
- Dynamic Virus Protection
- Optional Files
  - Communication System
  - ☒ NetWare Reporting
  - Scheduled Scan
  - Scheduled Update
- Product Documentation

Description: Installs the files that are required to perform scheduled virus scans.

< Back | Next > | Cancel

Set Feature Installation States Dialog Box – Subfeatures Displayed

- **Command AntiVirus Scanner** – installs the files that are required to perform on-demand virus scans. This feature is installed by default.

  The Command AntiVirus Scanner contains the following subfeatures:

  - **Help Files** – installs the Command AntiVirus online help files. By default, this subfeature is installed the first time it is accessed.
  - **Shell Extension** – adds the Command AntiVirus Scan option to the shell shortcut menu. This subfeature is installed by default.

- **Dynamic Virus Protection** – installs the files that are required to perform on-access virus scans. This feature is installed by default.

- **Optional Files** – installs the files that are required for additional Command AntiVirus features. This feature is installed by default.

Optional Files contains the following subfeatures:

- **Communication System** – installs the files that are required by CSS Central to remotely administer computers that are running Command AntiVirus. This subfeature is installed by default.
- **NetWare Reporting** – installs the files that are required for a workstation to communicate with a server that is running Command AntiVirus for NetWare. This subfeature is **not** installed by default.

NOTE: For **NetWare Reporting** to work, the Novell® NetWare® client **must** be installed.

- **Scheduled Scan** – installs the files that are required to perform scheduled virus scans. This subfeature is installed by default.
- **Scheduled Update** – installs the files that are required to perform a scheduled update. This subfeature is installed by default.

- **Product Documentation** – installs the README.TXT and the Command AntiVirus Multi-Platform Quick Start Guide. This feature is installed by default.

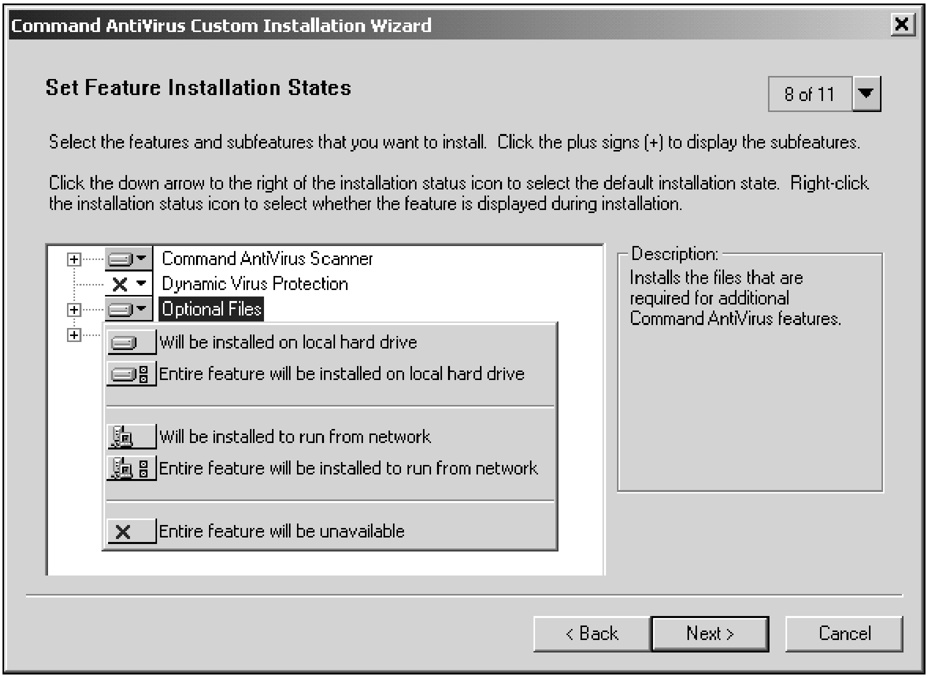
  Product Documentation contains the following subfeatures:

  - **Quick Start** – installs the Command AntiVirus Multi-Platform Quick Start Guide. This subfeature is installed by default.

    The guide, which is located in the file called MQCKST.PDF, provides a brief overview of our products and basic start-up instructions. It can be viewed with Adobe® Acrobat® Reader.

  - **Readme File** – installs the README.TXT file that contains the latest information on product enhancements, fixes and special instructions. This subfeature is installed by default.

To the left of each feature and subfeature is an icon that represents the present installation state. To view the explanation of each icon or to select a different installation state, click the down arrow ▾ to the right of the icon. The system displays a drop-down menu:



Command AntiVirus Custom Installation Wizard

Set Feature Installation States

8 of 11

Select the features and subfeatures that you want to install. Click the plus signs (+) to display the subfeatures.

Click the down arrow to the right of the installation status icon to select the default installation state. Right-click the installation status icon to select whether the feature is displayed during installation.

Command AntiVirus Scanner
Dynamic Virus Protection
Optional Files
Will be installed on local hard drive
Entire feature will be installed on local hard drive
Will be installed to run from network
Entire feature will be installed to run from network
Entire feature will be unavailable

Description:
Installs the files that are required for additional Command AntiVirus features.

Set Feature Installation States Dialog Box – Drop-down Menu

NOTE: When the installation state of a subfeature is different from the state of the feature, the icon of the feature has a gray background.

Depending on the feature or subfeature that you select, the drop-down menu contains all or some of the following items:

Will be installed on local hard drive – installs the selected feature or subfeature on the local hard drive. If you select a subfeature, this option also installs the parent feature. For example, if you select to install the online **Help Files**, the **Command AntiVirus Scanner** is also installed.

Entire feature will be installed on local hard drive – installs the selected feature and all of its subfeatures on the local hard drive. For example, if you select the **Command AntiVirus Scanner**, the **Help Files** and the **Shell Extension** are also installed.

If you select a subfeature, this option installs the parent feature and the selected subfeature. For example, if you select to install **NetWare Reporting**, **Optional Files** is also installed.

Will be installed to run from network – installs the selected feature or subfeature on a network drive.

If you select a subfeature, this option also installs the parent feature. For example, if you select to install the online **Help Files**, the **Command AntiVirus Scanner** is also installed.

Entire feature will be installed to run from network – installs the selected feature and all of its subfeatures on a network drive.

If you select a subfeature, this option also installs the parent feature. For example, if you select to install **NetWare Reporting**, **Optional Files** is also installed.

Feature will be installed when required – installs the selected feature the first time it is accessed. For example, if you select this option for the online **Help Files, Help** is installed only the first time it is used.

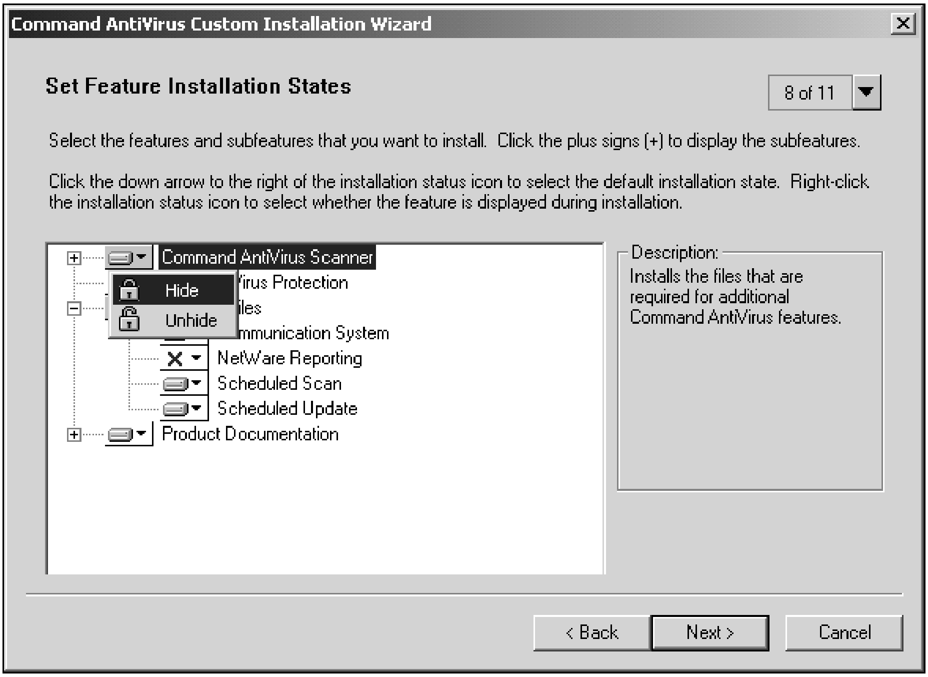
NOTE: You **<u>must</u>** have Windows Desktop Update installed to be able to use the **Feature will be installed when required** installation state. Active Desktop does not have to be enabled.

Entire feature will be unavailable – does **<u>not</u>** install the selected feature or any of its subfeatures.

To change the installation status for a selected feature or subfeature, click the appropriate icon. The program returns to the **Select Features** dialog box which now shows the installation status icon that you selected.

You can also select whether the feature is displayed during the installation process and when the user is adding or removing features after CSAV is installed.

Right-click the down arrow ▾ to the right of the installation state icon of a feature or subfeature. The system displays a drop-down menu:



Set Feature Installation States

Select the features and subfeatures that you want to install. Click the plus signs (+) to display the subfeatures.

Click the down arrow to the right of the installation status icon to select the default installation state. Right-click the installation status icon to select whether the feature is displayed during installation.

Description: Installs the files that are required for additional Command AntiVirus features.

Set Feature Installation States Dialog Box – Hide/Unhide Drop-down Menu

Select **<u>one</u>** of the following:

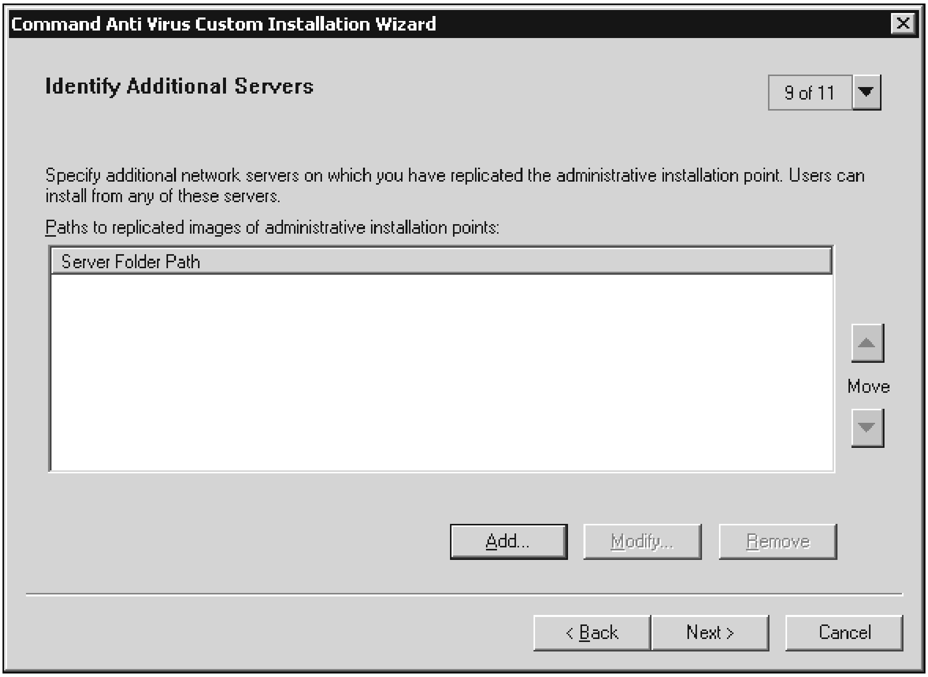
- **Hide –** The feature is **<u>not</u>** displayed during the installation process and when the user is adding or removing features in the Command AntiVirus installation program's **Add/Remove Application** dialog box. For more information, refer to **Installation Maintenance** in the ***Installation*** chapter.

The feature is only hidden. It is installed and available to the user unless you set the installation state to **Entire feature will be unavailable**.

NOTE: If you hide a feature, then all of the subfeatures are also hidden.

- **Unhide** – The feature is displayed during the installation process and when the user is adding or removing features after CSAV is installed. This is the default.

25. Click **Next**. The system displays the **Identify Additional Servers** dialog box:



Command Anti Virus Custom Installation Wizard
Identify Additional Servers
9 of 11

Specify additional network servers on which you have replicated the administrative installation point. Users can install from any of these servers.

Paths to replicated images of administrative installation points:

Server Folder Path

Move
Add...
Modify...
Remove
< Back
Next >
Cancel

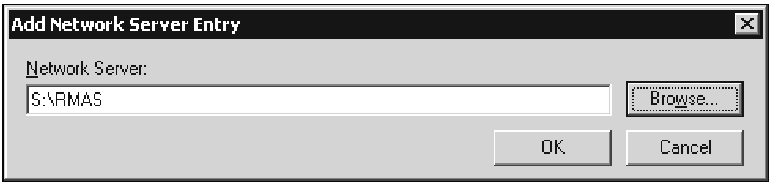
Identify Additional Servers Dialog Box

This dialog box allows you to specify additional network servers that have a copy of the installation folder tree. If you install features to run from the server or to be installed when the feature is first accessed, this option ensures that there is always access to an available network server.

Initially, the primary server is the server from which you installed Command AntiVirus. If this server is unavailable, an attempt is made to connect to each server in the list from top to bottom until a successful connection is made. If a connection is successful, the server that is connected now becomes the primary server.

If no server is available, the system prompts the user for the location of a server.

26. To add an additional network server, click **Add**. The system displays the **Add Network Server Entry** dialog box:



Add Network Server Entry

Network Server: S:\RMAS

Add Network Server Entry Dialog Box

27. In the **Network Server** text box, type the path and name of the server that you want to add, for example:

```
S:\AnnT\RMAS
```

The drive letter **<u>must</u>** be mapped on the user's computer. You can also specify a Universal Naming Convention (UNC) path.

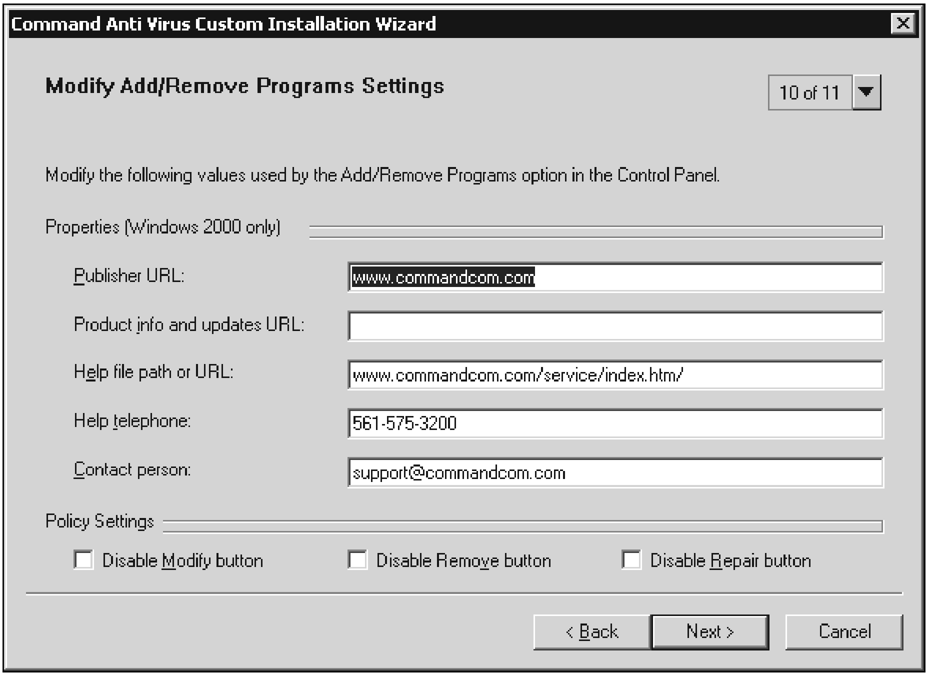
NOTE: Make sure that you type in a **<u>valid</u>** path and name. You can use the **Browse** button to search for the server.

28. Click **OK**. The system returns to the **Identify Additional Servers** dialog box. The **Server Folder Path** list box now contains the server that you added.

    Repeat **Steps 26** through **28** for each additional server that you want to add.

NOTE: To change a server, select a server in the list and click **Modify.** To delete a server, select a server in the list and click **Remove.** To change the position of a server in the list, select the server and click the up or down **Move** buttons.

29. Click **Next.** The system displays the **Modify Add/Remove Programs Settings** dialog box:



Modify Add/Remove Programs Settings

Modify the following values used by the Add/Remove Programs option in the Control Panel.

Properties (Windows 2000 only)

Publisher URL: www.commandcom.com

Product info and updates URL:

Help file path or URL: www.commandcom.com/service/index.htm/

Help telephone: 561-575-3200

Contact person: support@commandcom.com

Policy Settings

☐ Disable Modify button ☐ Disable Remove button ☐ Disable Repair button

Modify Add/Remove Programs Settings Dialog Box

This dialog box allows you to modify the information that is displayed in the Windows **Support Info** dialog box for Command AntiVirus. You can access this information through the Windows **Add/Remove Programs** dialog box in the Control Panel. Select Command AntiVirus and click **support information**.

You can also disable the **Change** and **Remove** buttons for Command AntiVirus that are displayed in the Windows **Add/Remove Programs** dialog box and the **Repair** button that is displayed in the Windows **Support Info** dialog box for Command AntiVirus.

30. To change the default contact information, type the new information in the appropriate text boxes.

31. To disable the following buttons, select or clear the appropriate check boxes under **Policy Settings**. These check boxes are **not** selected by default.

    - **Disable Modify button** – Allows you to prevent the users from modifying Command AntiVirus. When this function is disabled, the **Change** button for Command AntiVirus that is displayed in the Windows **Add/Remove Programs** dialog box is dimmed.

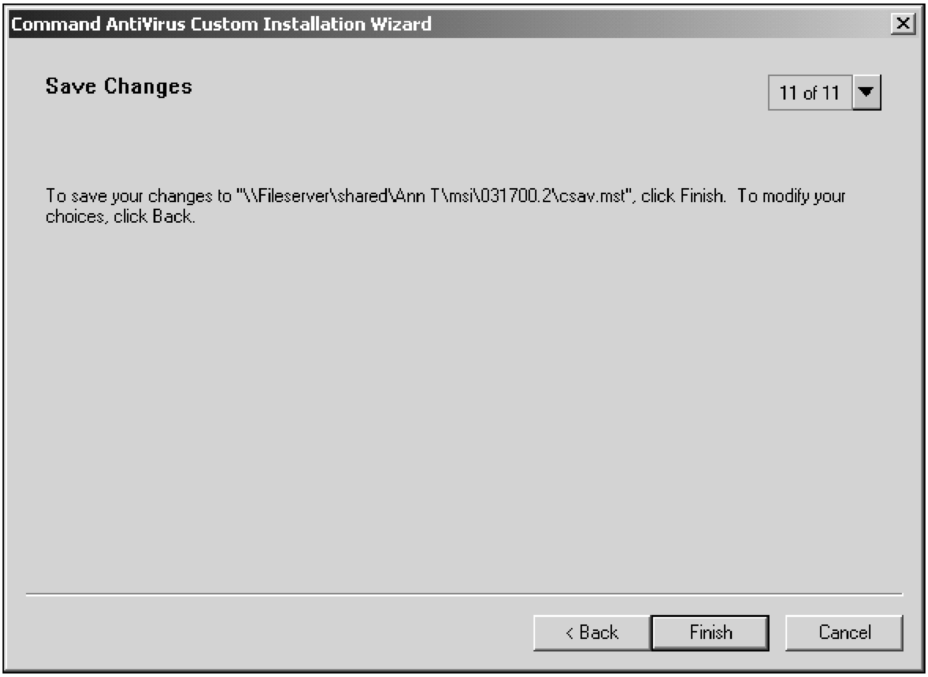
      For more information on making changes to Command AntiVirus after installation, refer to **Installation Maintenance** in the ***Installation*** chapter.

    - **Disable Remove button** – Allows you to prevent the users from removing Command AntiVirus through the Windows **Add/Remove Programs** dialog box. When this function is disabled, the **Remove** button for Command AntiVirus that is displayed in the Windows **Add/Remove Programs** dialog box is dimmed.

      For more information on removing Command AntiVirus through the Command AntiVirus installation program's **Add/Remove Application** dialog box, refer to **Installation Maintenance** in the ***Installation*** chapter.

    - **Disable Repair button** – Allows you to prevent the users from reinstalling Command AntiVirus through the Windows **Support Info** dialog box for Command AntiVirus. When this function is disabled, the **Repair** button is dimmed.

32. Click **Next**. The system displays the **Save Changes** dialog box:

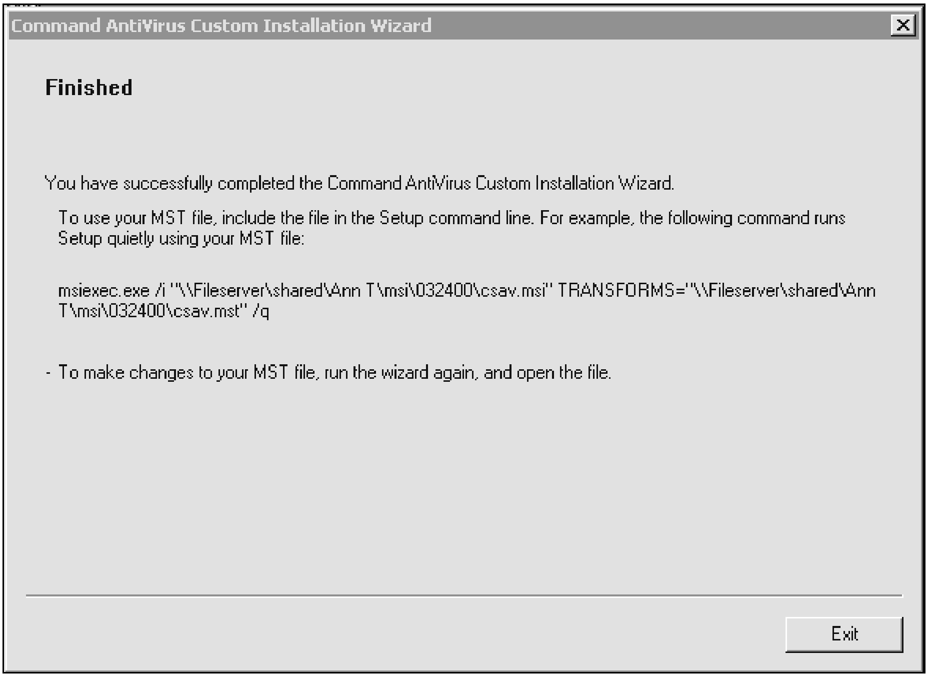


To save your changes to "\\Fileserver\shared\Ann T\msi\031700.2\csav.mst", click Finish. To modify your choices, click Back.

Save Changes Dialog Box

33. Click **Finish** to save your changes to the specified file. The system displays the **Finished** dialog box.

NOTE: If you need to modify your choices, click **Back**.



You have successfully completed the Command AntiVirus Custom Installation Wizard.

To use your MST file, include the file in the Setup command line. For example, the following command runs Setup quietly using your MST file:

```
msiexec.exe /i "\\Fileserver\shared\Ann T\msi\032400\csav.msi" TRANSFORMS="\\Fileserver\shared\Ann T\msi\032400\csav.mst" /q
```

- To make changes to your MST file, run the wizard again, and open the file.

Finished Dialog Box

34. Click **Exit** to end the program.

If you want to make changes to an MST file, run the Command AntiVirus Custom Installation Wizard again, and open the MST file.

NOTE: For information on deploying your customized installation of Command AntiVirus to multiple users over the network, refer to **Deploying Command AntiVirus through Group Policy** located later in this chapter.

DEPLOYING COMMAND ANTIVIRUS THROUGH GROUP POLICY

You can use Group Policy on computers running Windows 2000 to deploy Command AntiVirus for Windows NT/2000 to individual computers from a central location on a network. This section provides information on:

- Configuring group policies for Command AntiVirus
- Assigning the installation package to computers
- Deploying updated Command AntiVirus definition files
- Deploying new versions of Command AntiVirus
- Removing Command AntiVirus for Windows NT/2000

GETTING STARTED

Consider the following Microsoft requirements before proceeding with the steps that are described in this section. For more information about Group Policy, refer to the documentation that came with your Windows 2000 operating system software.

- To set Group Policy or Software Installation snap-ins for a domain, you must use a computer that is configured as a domain controller.
- To set policies for users of a particular computer, you must be an administrator for that computer or have equivalent rights.
- To set policies for an organizational unit in a domain, you must be an administrator for that domain or have equivalent rights.

Group Policy-based deployment simplifies software installation and maintenance of assigned applications. Through Windows 2000 Group Policy, you can distribute Command AntiVirus for Windows NT/2000 by the following method:

- **Assigning applications to computers –** Installs the next time the computer is started.

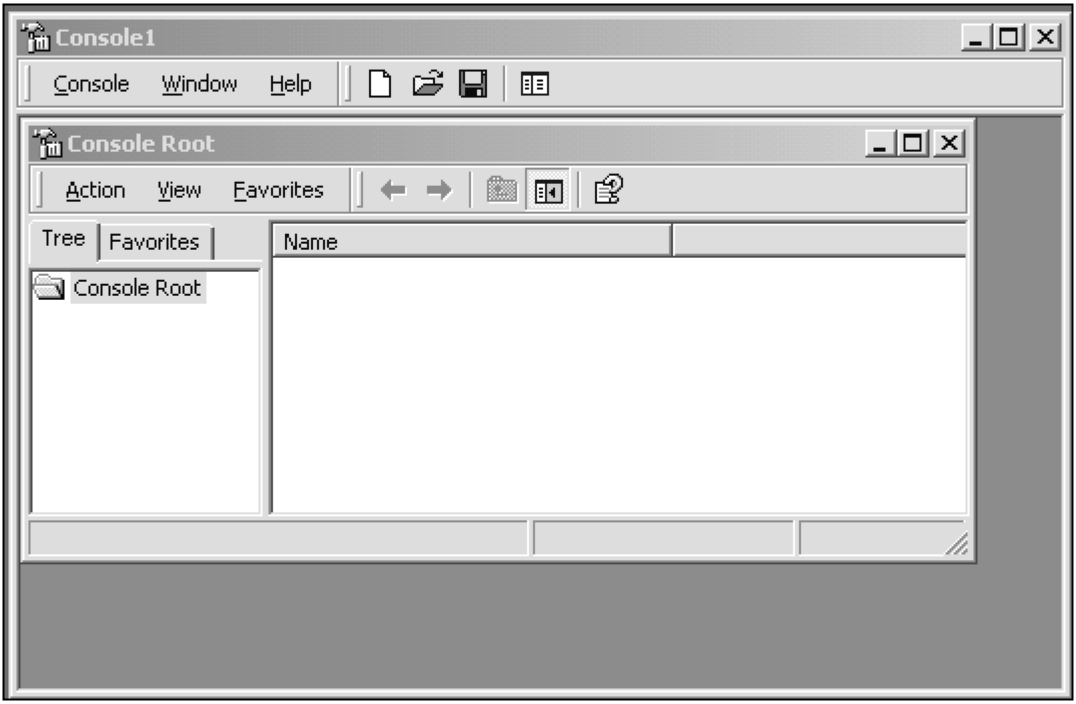
CONFIGURING GROUP POLICIES

Before you can install Command AntiVirus for Windows NT/2000 onto individual computers from a central location on a network, you must open the Software Installation snap-in and create a Group Policy object for the group of users, computers, or domains (including domain servers) that you want to target during deployment. You can then save your selections for future use by creating a Microsoft Management Console (MSC file). The following information will help you through this process.

NOTE: For more information on installing Command AntiVirus for Windows NT/ 2000 to a central location on a network, refer to **Installing Command AntiVirus to a Software Distribution point (SDP)** located previously in this chapter.

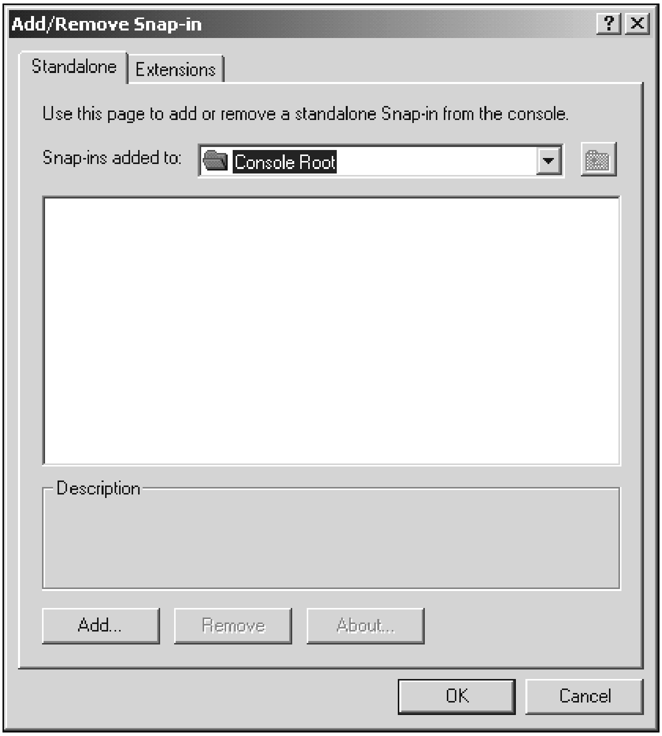
To configure group policies for Command AntiVirus for Windows NT/2000 follow these steps:

1. Click the **Start** button on the Windows task bar.
2. Click **Run**.
3. In the text box, type **mmc**.
4. Click **OK**. The system displays the **Microsoft Management Console**:



Microsoft Management Console

5. From the **Console** drop-down menu, select **Add/Remove Snap-in....** The system displays the **Add/Remove Snap-in** dialog box:

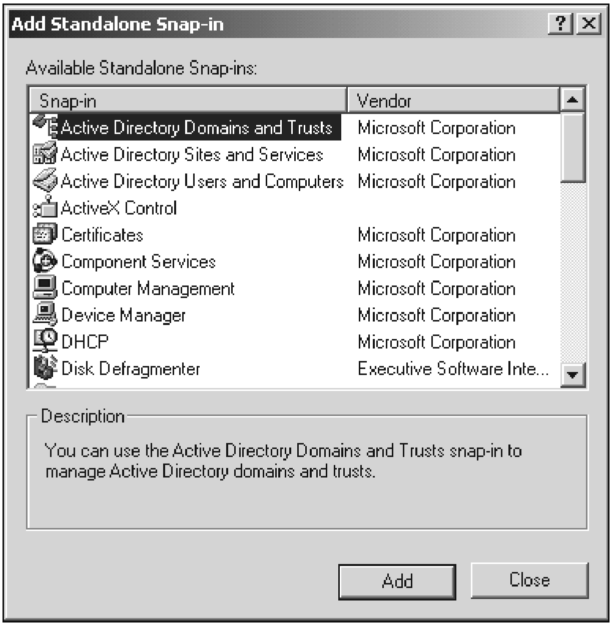


Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Add/Remove Snap-in Dialog Box

6. Click **Add**. The system displays the **Add Standalone Snap-in** dialog box:



Available Standalone Snap-ins:

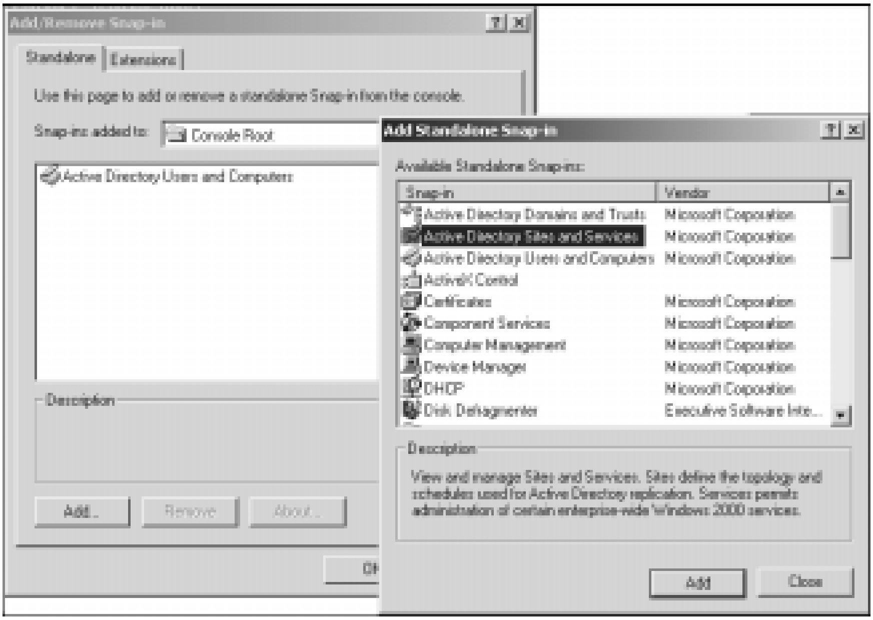
Snap-in	Vendor
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Computers	Microsoft Corporation
ActiveX Control	
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
DHCP	Microsoft Corporation
Disk Defragmenter	Executive Software Inte...

Description

You can use the Active Directory Domains and Trusts snap-in to manage Active Directory domains and trusts.

Add Standalone Dialog Box

7. From the **Add Standalone Snap-in** list, select **Active Directory Users and Computers** and click **Add.** This item is now added to the **Add/Remove Snap-in** list:



Add/Remove Snap-in

Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Active Directory Users and Computers

Description

Add Standalone Snap-in

Available Standalone Snap-ins:

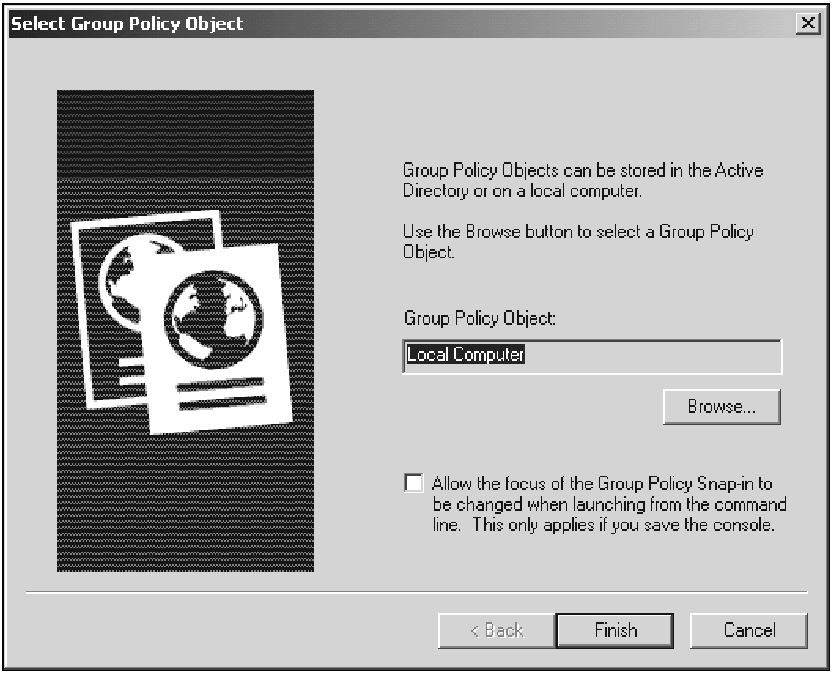
Snap-in	Vendor
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Computers	Microsoft Corporation
ActiveX Control	
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
DHCP	Microsoft Corporation
Disk Defragmenter	Executive Software Inte...

Description

View and manage Sites and Services. Sites define the topology and schedules used for Active Directory replication. Services permit administration of certain enterprise-wide Windows 2000 services.

Add/Remove Snap-in Dialog Box and Add Standalone Snap-in List

8. From the **Add Standalone Snap-in** list, select **Active Directory Sites and Services** and click **Add**. This item is now added to the **Add/Remove Snap-in** list.
9. From the **Add Standalone Snap-in** list, select **Group Policy** and click **Add**. The system displays the **Select Group Policy Object** dialog box:



Select Group Policy Object

Group Policy Objects can be stored in the Active Directory or on a local computer.

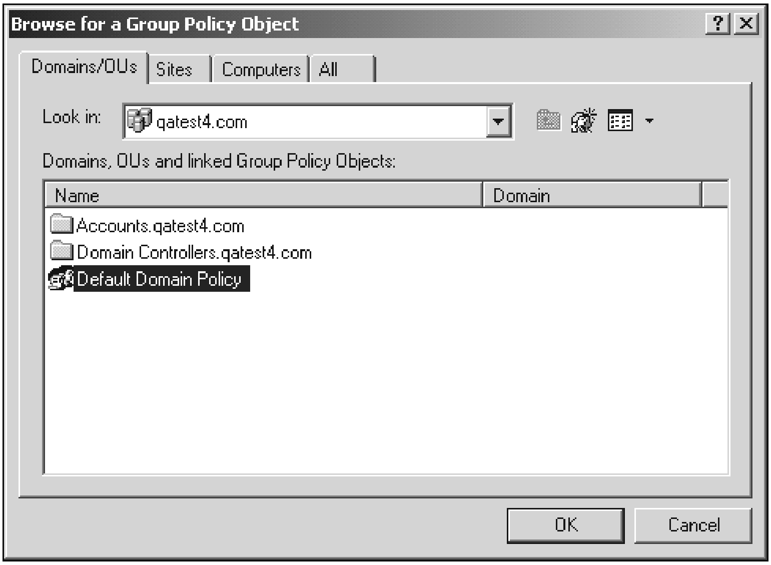
Use the Browse button to select a Group Policy Object.

Group Policy Object: Local Computer

□ Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.

Select Group Policy Object Dialog Box

10. Click **Browse** to select a Group Policy object. The system displays the **Browse for a Group Policy Object** dialog box:



Browse Group Policy Object Dialog Box

11. From the **Domains/OUs**, **Sites**, **Computers**, or **All** tab, select the Group Policy object for the group of users, computers, or domains (including domain servers) that you want to target during deployment.

    If you need to create a new Group Policy object for your selected group, right-click in the list box. The system displays a drop-down menu. Click **New**. Then, in the text box that is now in the **Name** list, type the name of the new Group Policy object and press **Enter**.

12. Click **OK**. The system returns to the **Select Group Policy Object** dialog box.

13. Click **Finish** to add your group policy to the **Add/Remove Snap-in** list. The system returns to the **Add Standalone Snap-in** dialog box.

    Repeat **Steps 9** through **13** to add additional group policies.

14. In the **Add Standalone Snap-in** dialog box, click **Close**.

15. In the **Add/Remove Snap-in** dialog box, click **OK**. The system returns to the **Microsoft Management Console**.

16. From the **Console** drop-down menu, select **Save As**. The system displays the **Save As** dialog box:

17. Type a name in the File name text box, for example:

    ```
    CSAVConsole.msc
    ```

18. Click **Save**.

    You are ready to assign Command AntiVirus for Windows NT/2000 to individual computers.

19. Proceed to **Assigning Command AntiVirus to Computers**.

ASSIGNING COMMAND ANTIVIRUS TO COMPUTERS

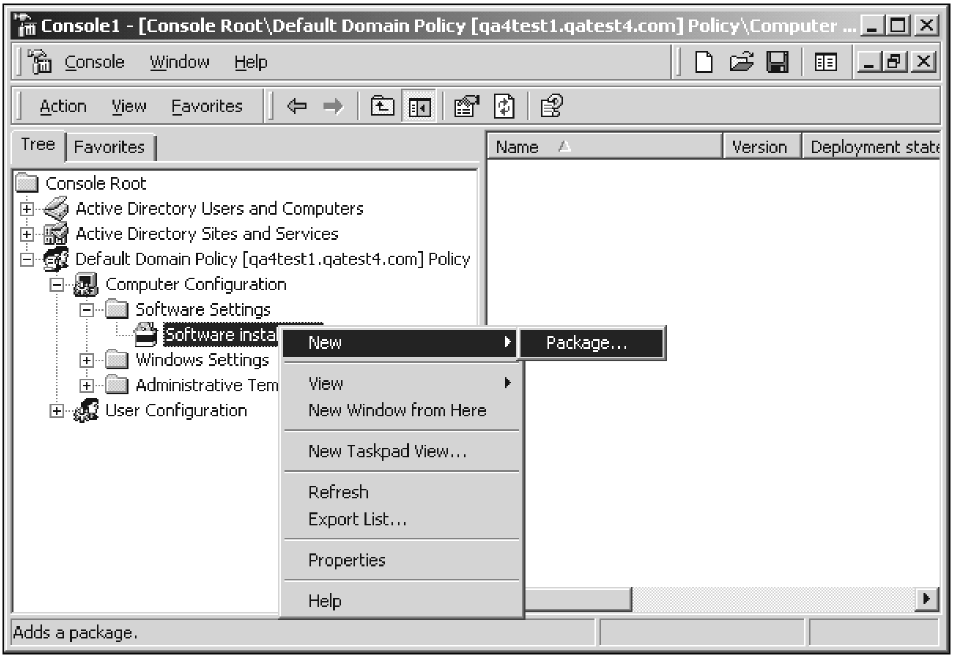
Assigning Command AntiVirus for Windows NT/2000 through **Computer Configuration** installs the program when the local computer is started.

NOTE: If you are deploying a custom installation, make sure that you have customized your settings through the Command AntiVirus Custom Installation Wizard. For more information, refer to **Customizing Your Installation Settings** located previously in this chapter.

To assign Command AntiVirus to computers, follow these steps:

1. In the **Console Root Tree** of the **Microsoft Management Console**, click the plus sign next to the Group Policy object that you selected for Command AntiVirus. This action expands this item. Then, expand **Computer Configuration** and **Software Settings**.

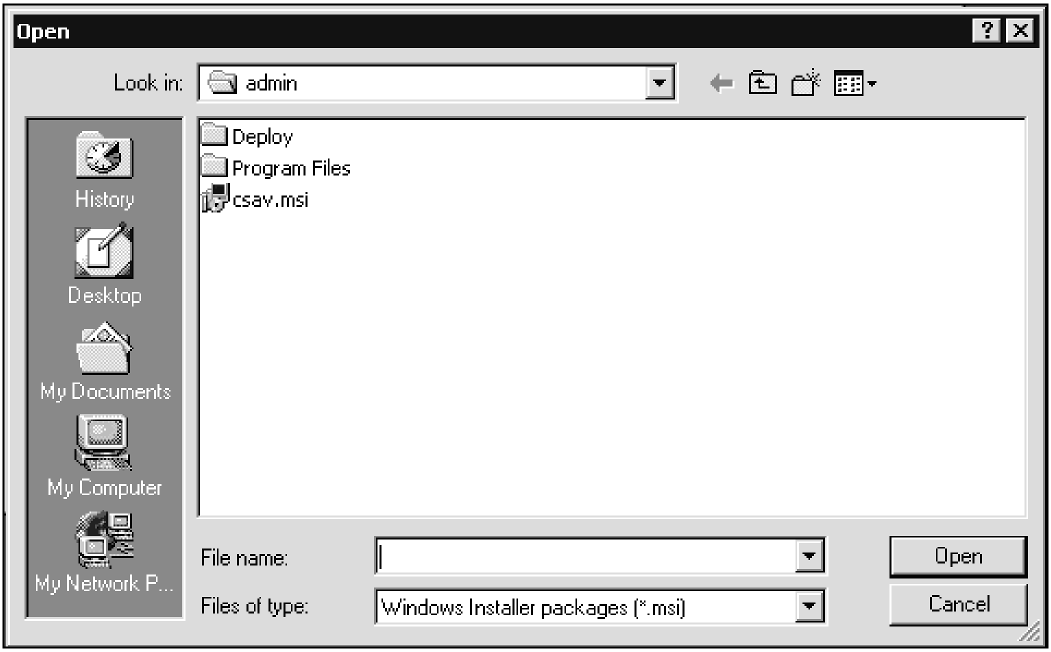
2. Right-click **Software Installation**. The system displays a drop-down menu:



Adds a package.

Software Installation Drop-down Menu

3. Select **New** and click **Package....** The system displays the **Open** dialog box:



Look in: admin

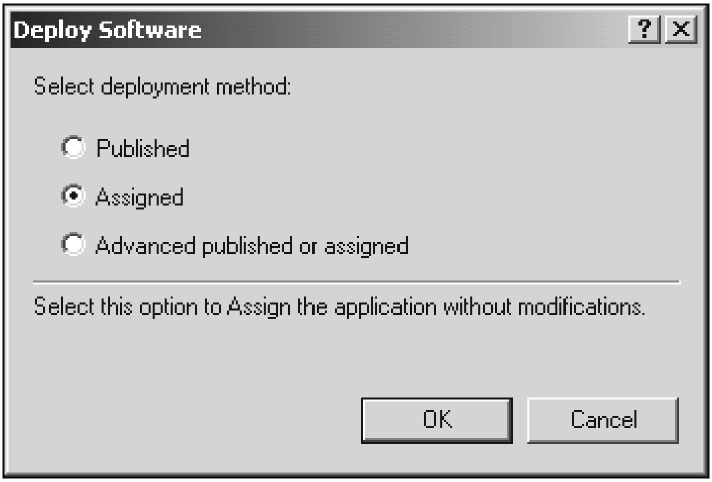
Deploy
Program Files
csav.msi

File name:

Files of type: Windows Installer packages (*.msi)

Open Dialog Box

4. Select the CSAV.MSI Windows installer package in the shared network folder and click **Open**. The system displays the **Deploy Software** dialog box:



Deploy Software

Select deployment method:

○ Published

● Assigned

○ Advanced published or assigned

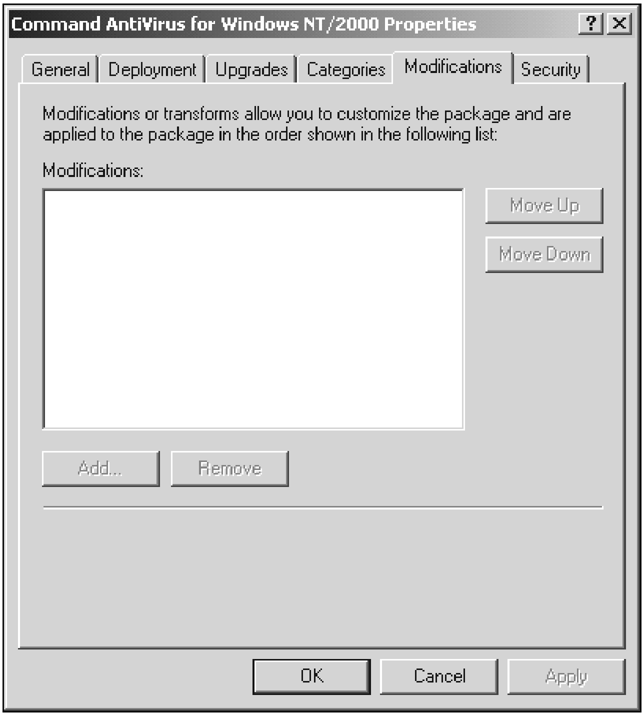
Select this option to Assign the application without modifications.

Deploy Software Dialog Box

5. If you are deploying a **Typical** installation, select **Assigned** and click **OK**. The system returns to the **Microsoft Management Console**. Your deployment is complete. Command AntiVirus will be installed onto the computers that you selected the next time the computers are started. You have finished this section.

   If you are deploying a **Custom** installation, proceed to **Step 6**.

6. Select **Advanced published or assigned** and click **OK**. The system displays the **Command AntiVirus for Windows NT/2000 Properties** dialog box.
7. Click the **Modifications** tab. The system displays the **Modifications** dialog box:



Modifications or transforms allow you to customize the package and are applied to the package in the order shown in the following list:

Modifications:

Modifications Dialog Box

8. Click **Add**. The system displays the **Open** dialog box.
9. Select the CSAV.MST file in the shared network folder and click **Open**. The system returns to the **Modifications** dialog box.

   Repeat **Steps 8** and **9** for all other MST files that you want to add.

NOTE: Do not click **OK** until you have added all MST files in their proper order. You can use the **Move Up** and **Move Down** buttons to change the order of the files.

10. Click **OK**. The system returns to the **Microsoft Management Console**.

Your deployment is complete. Command AntiVirus will be installed onto the computers that you selected the next time the computers are started.

UPDATING DEFFILES

To provide protection against new viruses, we update the Command AntiVirus definition files (deffiles) frequently. You can download the file called DEFMSP.EXE from the Command Software web site at www.commandcom.com. DEFMSP.EXE is a self-extracting file that contains the latest deffiles patch (.MSP). You can then distribute the patch through Group Policy onto the computers that were specified in the original deployment configuration.

We recommend that you perform an administrative installation of the deffiles patch to your software distribution points (SDPs). This allows you to apply and distribute the patch easily through Group Policy.

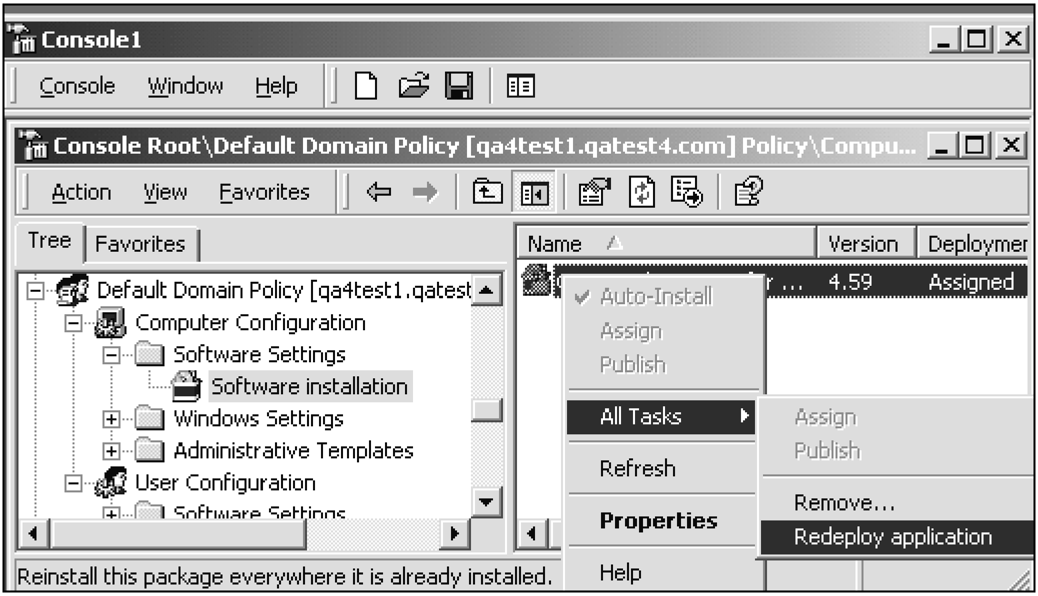
To perform an administrative installation of the deffiles patch, at the command line, type the following and press **Enter**.

```
msiexec /a csav.msi /p csav.msp
```

NOTE: Be sure to select the same network path that you used for the original SDP. The name of the CSAV MSP file changes with each update.

To distribute the deffiles patch follow these steps:

1. In the **Console Root Tree** of the **Microsoft Management Console**, click the plus sign next to the Group Policy object that you selected for Command AntiVirus. This action expands this item. Then, expand **Computer Configuration** and **Software Settings**.
2. Click **Software Installation**. The right-hand pane now lists Command AntiVirus.
3. Right-click **Command AntiVirus**. The system displays a drop-down menu:



Reinstall this package everywhere it is already installed.

Package Drop-down Menu – All Tasks

4. Select **All Tasks** and click **Redeploy application**. The system displays a dialog box asking you if you want to continue.
5. Click **Yes**.

Your redeployment is complete. Command AntiVirus with the updated deffiles will be reinstalled onto the computers that were specified in the original deployment configuration the next time the computers are started.

UPGRADING COMMAND ANTIVIRUS

We recommend that you perform an administrative installation of the Command AntiVirus upgrade package to your software distribution points (SDPs). This allows you to easily apply and distribute the upgrade through Group Policy onto the computers that were specified in the original deployment configuration. For more information, refer to **Installing Command AntiVirus To a Software Distribution point (SDP)** located previously in this chapter.

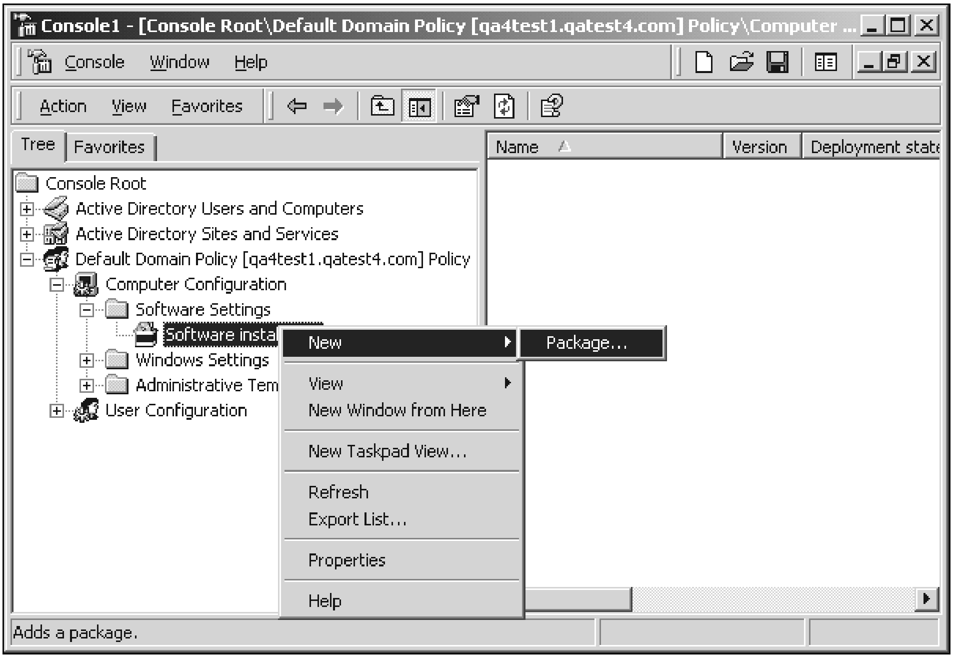
If you want to customize the installation features and settings of the Command AntiVirus upgrade package, you must create a custom Windows installer transform (MST file) before you install the upgrade. For more information, refer to **Customizing Your Installation Settings** located previously in this chapter.

Adding the Command AntiVirus Upgrade Package to Group Policy

Before you can install the Command AntiVirus upgrade, you must add the upgrade package and any MST files that you have created for the upgrade to the group policy that you selected for Command AntiVirus.

To add the Command AntiVirus upgrade package to the selected group policy, follow these steps:

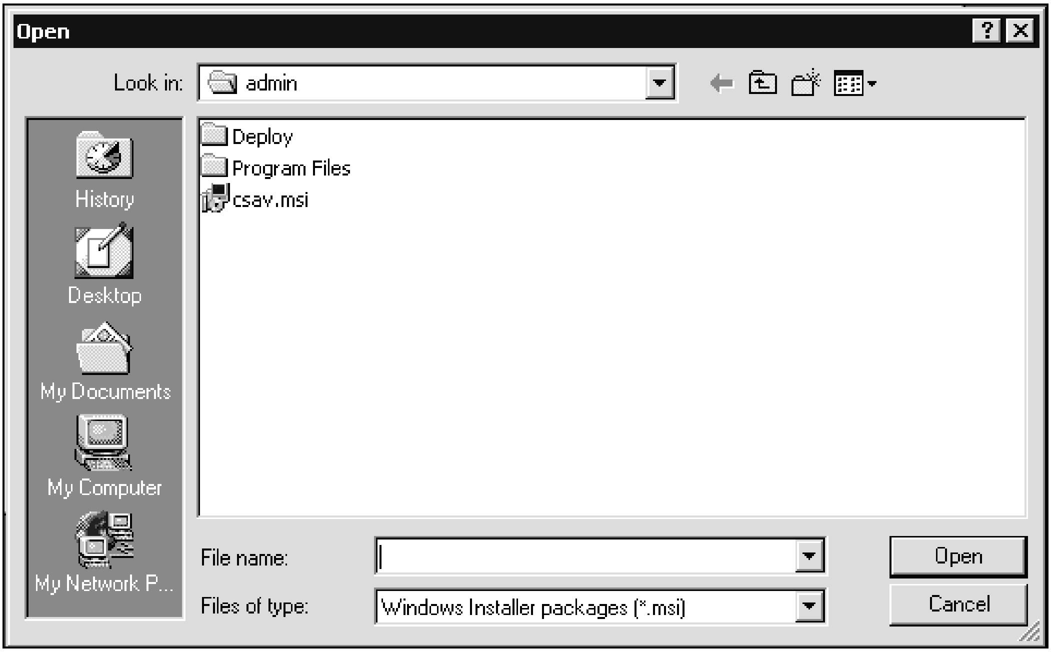
1. In the **Console Root Tree** of the **Microsoft Management Console**, click the plus sign next to the Group Policy object that you selected for Command AntiVirus. This action expands this item. Then, expand **Computer Configuration** and **Software Settings**.
2. Right-click **Software Installation**. The system displays a drop-down menu:



Adds a package.

Software Installation Drop-down Menu

3. Select **New** and click **Package....** The system displays the **Open** dialog box:



Open

Look in: admin

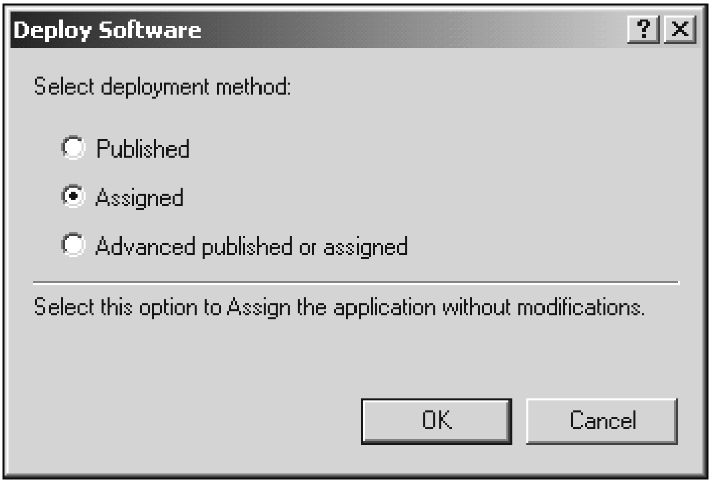
Deploy
Program Files
csav.msi

File name:

Files of type: Windows Installer packages (*.msi)

Open Dialog Box

4. Select the CSAV.MSI Windows installer upgrade package in the shared network folder and click **Open**. The system displays the **Deploy Software** dialog box:



Deploy Software

Select deployment method:

○ Published

● Assigned

○ Advanced published or assigned

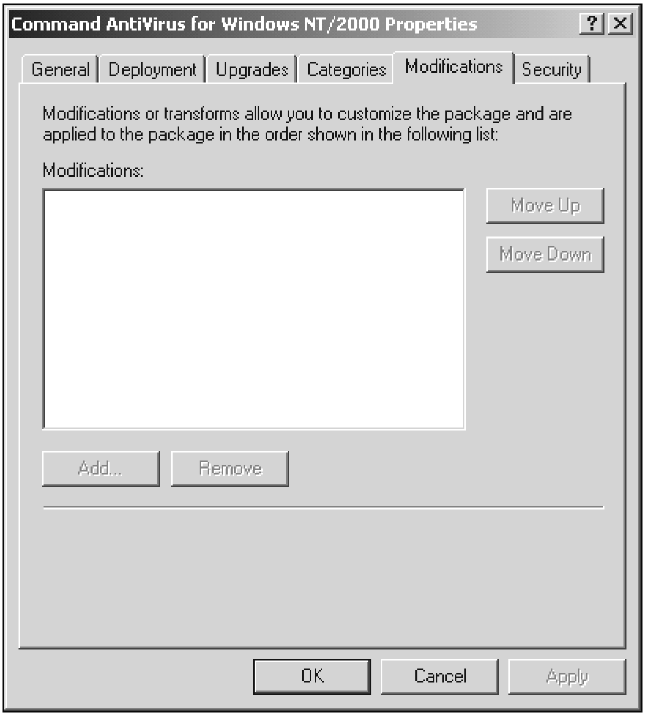
Select this option to Assign the application without modifications.

Deploy Software Dialog Box

5. If you are deploying a **Typical** installation, select **Assigned** and click **OK**. The system returns to the **Microsoft Management Console**. Your deployment is complete. Command AntiVirus will be installed to the computers that you have selected the next time the computer is started.

   If you are deploying a **Custom** installation, select **Advanced published or assigned** and click **OK**. The system displays the Command AntiVirus for Windows NT/2000 Properties dialog box.

6. Click the **Modifications** tab. The system displays the **Modifications** dialog box:



Command AntiVirus for Windows NT/2000 Properties

Modifications or transforms allow you to customize the package and are applied to the package in the order shown in the following list:

Modifications:

Modifications Dialog Box

7. Click **Add**. The system displays the **Open** dialog box.
8. Select the CSAV.MST file for the upgrade package in the shared network folder and click **Open**. The system returns to the **Modifications** dialog box.

   Repeat **Steps 7** and **8** for all other MST files that you want to add.

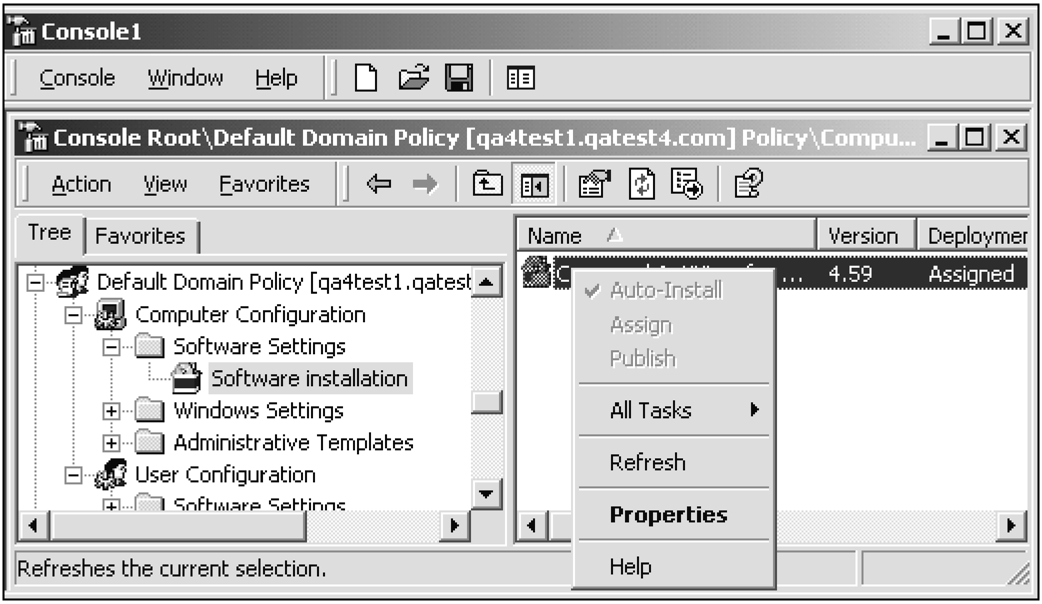
NOTE: Do not click **OK** until you have added all MST files in their proper order. You can use the **Move Up** and **Move Down** buttons to change the order of the files.

9. Click **OK**. The system returns to the **Microsoft Management Console**.
10. Proceed to **Distributing the Command AntiVirus Upgrade Package**.

Distributing the Command AntiVirus Upgrade Package

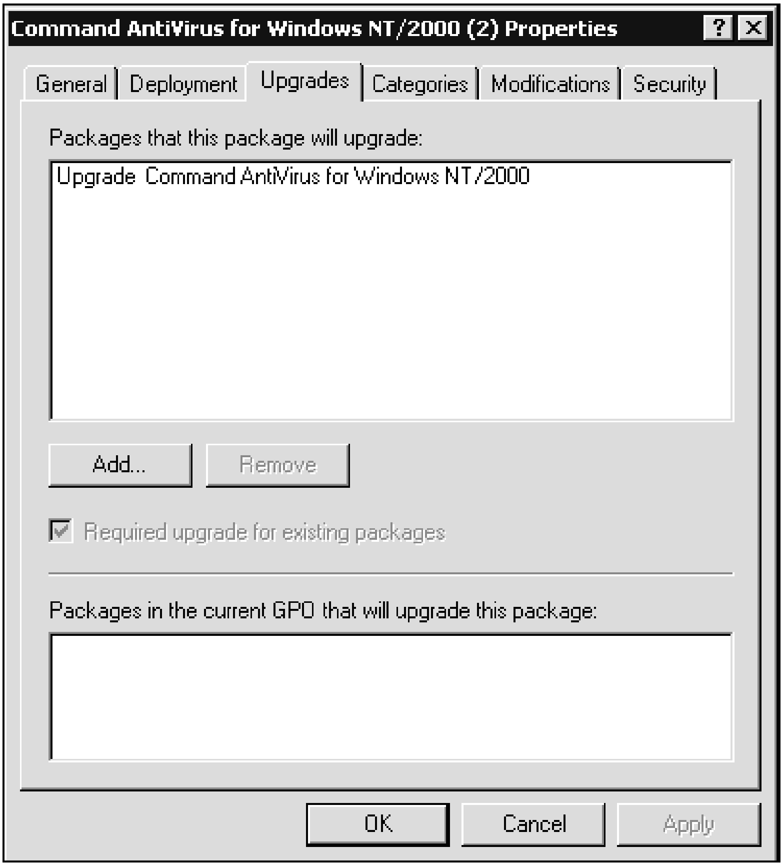
To distribute the Command AntiVirus upgrade follow these steps:

1. In the **Console Root Tree** of the **Microsoft Management Console**, click the plus sign next to the Group Policy object that you selected for Command AntiVirus. This action expands this item. Then, expand **Computer Configuration** and **Software Settings**.
2. Double-click **Software Installation**. The right-hand pane now lists the original Command AntiVirus package and the upgrade package.
3. Right-click the **Command AntiVirus upgrade package**. The system displays a drop-down menu:



Package Drop-down Menu

4. Click **Properties**. The system displays the **Command AntiVirus for Windows NT/2000 (2) Properties** dialog box.
5. Click the **Upgrades** tab. The system displays the **Upgrades** dialog box:



Packages that this package will upgrade:

Upgrade Command AntiVirus for Windows NT/2000

☑ Required upgrade for existing packages

Packages in the current GPO that will upgrade this package:

Upgrades Dialog Box

6. In the **Packages that this package will upgrade** list, select **Upgrade Command AntiVirus for Windows NT/2000**.
7. If you want to require users to upgrade to the new package, select the **Required upgrade for existing packages** check box.
8. Click **OK**.

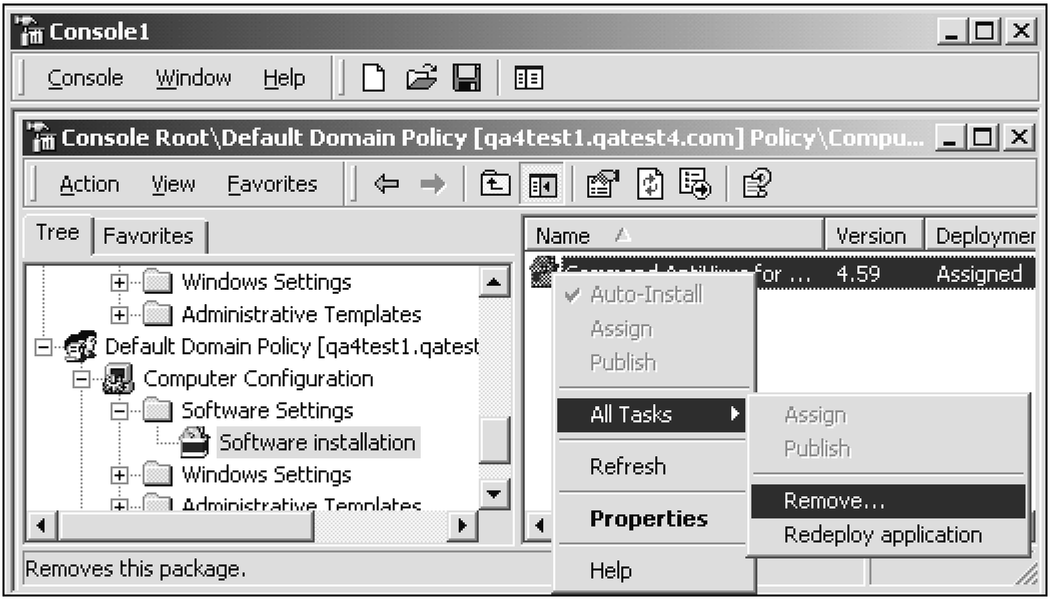
Your deployment is complete. The upgraded version of Command AntiVirus will be reinstalled to the computers that were specified in the original deployment configuration the next time the computer is started.

REMOVING COMMAND ANTIVIRUS

You can also use Group Policy to remove Command AntiVirus for Windows NT/ 2000 from individual computers on your network or to stop installing it on to new computers.

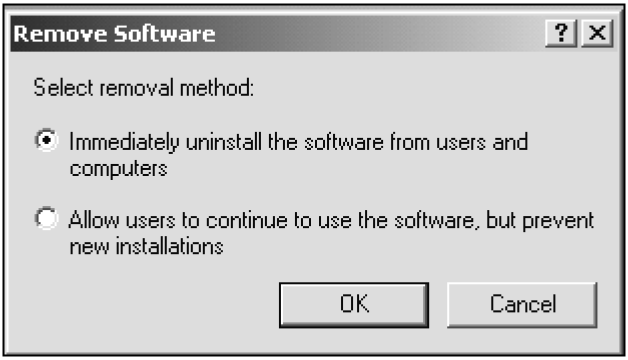
To remove or to stop the installation of Command AntiVirus for Windows NT/2000 follow these steps:

1. In the **Console Root Tree** of the **Microsoft Management Console**, click the plus sign next to the Group Policy object that you selected for Command AntiVirus. This action expands this item. Then, expand **Computer Configuration** and **Software Settings**.
2. Double-click **Software Installation**. The right-hand pane now lists Command AntiVirus.
3. Right-click **Command AntiVirus**. The system displays a drop-down menu:



Package Drop-down Menu – All Tasks

4. Select **All Tasks** and click **Remove.** The system displays the **Remove Software** dialog box:


Remove Software

Select removal method:

● Immediately uninstall the software from users and computers

○ Allow users to continue to use the software, but prevent new installations

Remove Software Dialog Box

5. Select **one** of the following removal methods and click **OK**:

   - **Immediately uninstall the software from users and computers** – Removes Command AntiVirus the next time the computer restarts.
   - **Allow users to continue to use the software, but prevent new installations** – Allows users who are currently using Command AntiVirus to continue using it and to perform repairs, but does not allow any new installations.

AUTOMATIC UPDATE

NOTE: Stand-alone (non-networked) users of Command AntiVirus can continue to use the standard installation method for updates as they will derive little benefit from this method.

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 workstation 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 also allows you to update an individual workstation on demand by using the **Update Now** button.

Automatic Update operates by placing Command AntiVirus files in a unique parent directory in a shared location on the network. When the user logs on to the computer, the automatic update process compares the dates (versions in CSAV for Windows NT/2000) of the files on the workstation with those on the server. If the server dates are newer, the workstations automatically update themselves 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.

In Command AntiVirus for Windows NT/2000, the user sees only a progress bar and error dialog boxes for both full-product and component updates.

Getting Started

NOTE: To use the Automatic Update feature in Command AntiVirus for Windows NT/2000, Command AntiVirus must be installed on each workstation. For new installations, you must run CSAV.MSI at the workstation or use Group Policy to roll out the new product.

NOTE: Once you complete the automatic update process, workstations are updated automatically each time you place **updated** files in the **automatic update directory** and its subdirectories. Updates occur at each login or if the user is logged on, at a preconfigured time. For example, the default time is between, 4 a.m. and 5 a.m.

F-AGENT (the yellow **C** in the lower right corner of the system tray) **must** be active for updates to occur automatically.

As soon as an update takes place, the program does **not** automatically update again for at least 24 hours.

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.
```

Creating the Automatic Update Directory

To create the **automatic update directory**, follow these steps:

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

   ```
   S:\NEWFPROT
   ```

2. Create a subdirectory for each platform to be updated. For example:

   ```
   S:\NEWFPROT\CSAV95
   ```

3. It is necessary to create subdirectories under each platform directory. These subdirectories will be used to contain full product, component updates, and definition 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\SIGN
   ```

4. Download and extract the latest update files, for example, the definition (.DEF) files.

5. Copy **all** of the product files into their respective subdirectory. For example, you would copy the definition files that you extracted in **Step 4** into the S:\NEWFPROT\CSAV95\SIGN subdirectory.

6. Using Notepad or any text editor, create a file named CSSFILES.INI in the root of the **automatic update directory**. 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\

[NT40_W-ANTIVIR]

BASEDIR=S:\NEWFPROT\CSAVNTW

FULLPROD=FULL\

COMPONT=COMP\

DEFFILES=SIGN\

[WIN2000_S-ANTIVIR]

BASEDIR=S:\NEWFPROT\CSAV2000S

FULLPROD=FULL\

COMPONT=COMP\

DEFFILES=SIGN\
[WIN2000_W-ANTIVIR]

BASEDIR=S:\NEWFPROT\CSAV2000W

FULLPROD=FULL\

COMPONT=COMP\

DEFFILES=SIGN\
```

If automatic updates are performed by multiple workstations over a network, the CSSFILES.INI file **must** use Universal Naming Convention (UNC) paths.

7. Save the changes to the CSSFILES.INI file.

   In Command AntiVirus for Windows NT/2000, use the Command AntiVirus Custom Installation Wizard to make changes to the Automatic Update settings in **Preferences**. You can also change the time the update takes place.

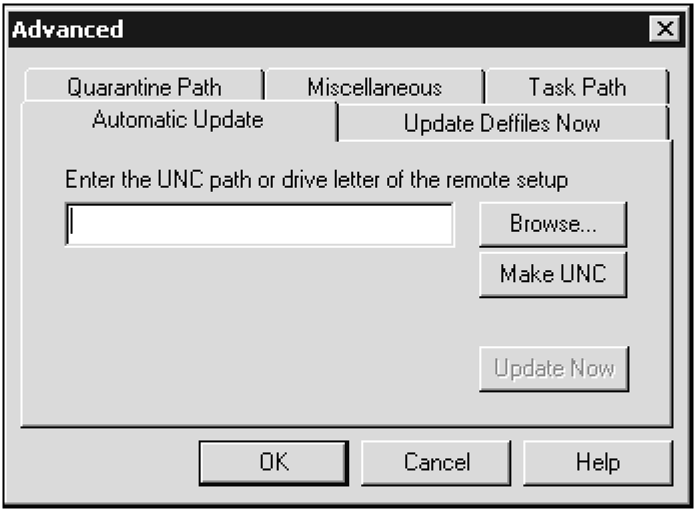
   Then, use Windows Group Policy to deploy the changes throughout the network. For more information, refer to **Customizing Your Installations** and **Deploying Command AntiVirus through Group Policy** located previously in this chapter.

Setting the Automatic Update Path Manually

In Command AntiVirus for Windows NT/2000 and Command AntiVirus for Windows NT, you must be a member of the local Administrators group to perform this task.

To set the path to the automatic update directory, follow these steps:

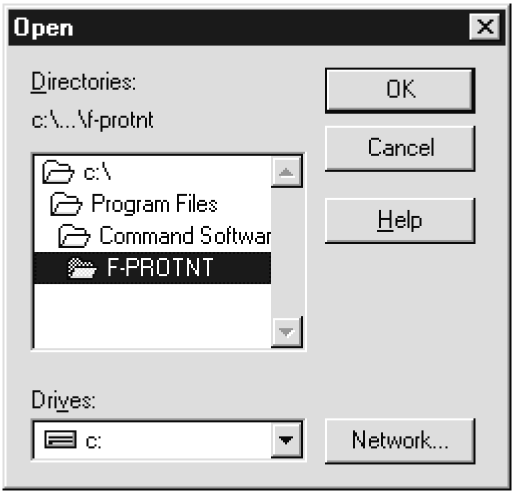
1. Open Command AntiVirus.
2. Click **Preferences**. The system displays a drop-down menu.
3. Click **Advanced**. The system displays the **Advanced** dialog box.
4. Click the **Automatic Update** tab. The system displays the **Automatic Update** dialog box:



Enter the UNC path or drive letter of the remote setup

Automatic Update Dialog Box

5. Click **Browse**. The system displays the **Browse Open** dialog box:



Browse Open Dialog Box

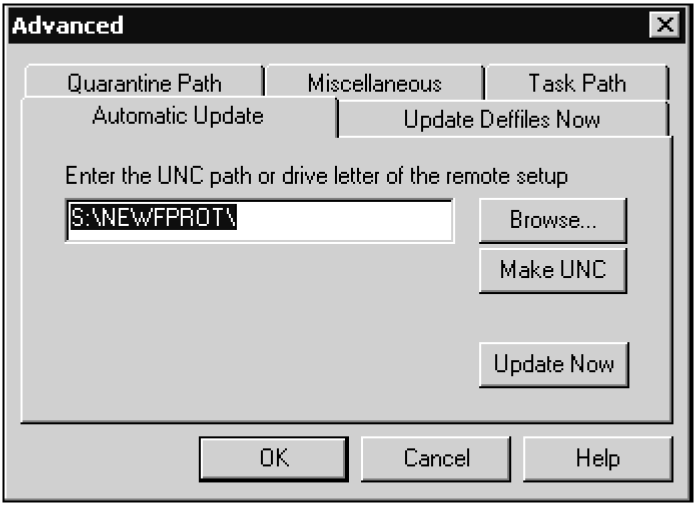
6. Select the drive\path of the **automatic update directory**. For example:

```
S:\NEWFPROT
```

The directory path **<u>must</u>** point to the **automatic update directory** which contains the CSSFILES.INI regardless of whether you are performing partial or full-product updates.

NOTE: If the drive is not mapped, click **Network**. Select the correct path and click **OK** to connect the drive. The system returns to the **Browse Open** dialog box.

7. Click **OK**. The system returns to the **Automatic Update** dialog box with the selected path entered in the text field.



Enter the UNC path or drive letter of the remote setup

S:\NEWFPROT\

Automatic Update Dialog Box

Be sure that you have entered the correct path to the **automatic update directory**. Updates will be made from the path that you have specified.

NOTE: When the drive\path selected is a network drive, use the **Make UNC** button to convert it to a Universal Naming Convention (UNC) path.

8. Click **OK**.

In Command AntiVirus for Windows 95/98, there are no restrictions to prevent the user from changing the path of the **automatic update directory**. If the user changes the path, the updates will be made from the path specified.

If you are administering CSAV on your network through CSS Central, you can prevent users from changing the **automatic update directory** path by locking the preferences on remote computers. For more information, refer to **Writing the New Preferences to the Remote System(s)** in the ***CSS Central*** chapter of the *Command AntiVirus Multi-Platform Quick Start Guide.*

In Command AntiVirus for Windows NT and Command AntiVirus for Windows NT/2000, the user **must** be assigned to a local Administrators group to change the **automatic update directory path** from the **Preferences** menu.

In Command AntiVirus for Windows NT/2000, you can also prevent the users from modifying the default settings for the items on the Command AntiVirus **Preferences** menu. For more information, refer to **Customizing Your Installation Settings** located previously in this chapter.

NOTE: To turn off the Automatic Update feature, leave the **automatic update directory** blank.

Using the Update Now Button

The **Update Now** button allows the user to update the individual workstation immediately.

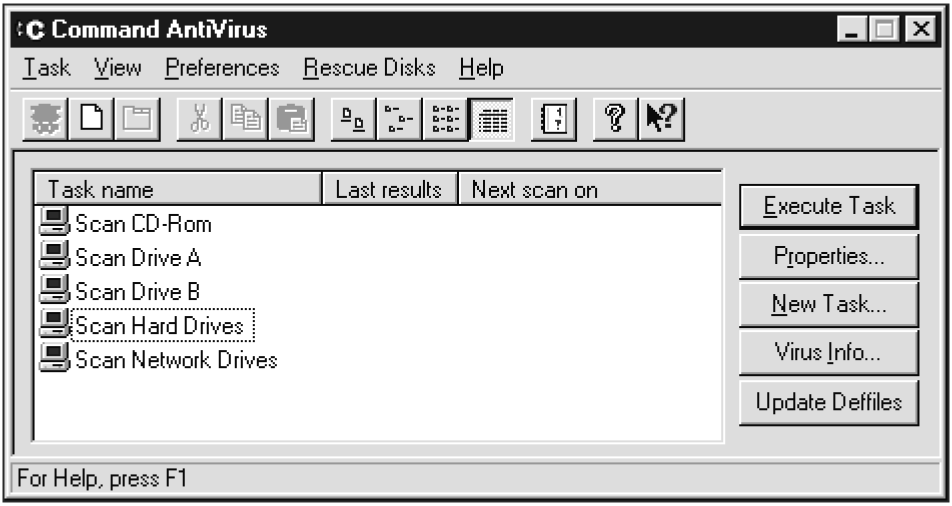
NOTE: In Command AntiVirus for Windows NT/2000 and Command AntiVirus for Windows NT, to use the **Update Now** button, the user **must** be a member of the local Administrators group.

DEFINITION FILES UPDATE BUTTON

This feature allows the user to update the Command AntiVirus definition files on-demand by using the **Update Deffiles** button on the **Command AntiVirus Main** dialog box.

NOTE: In Command AntiVirus for Windows NT/2000, for the user to use the **Update Deffiles** button, **one** of the following conditions **must** be met:

- The user is a member of the local Administrators group
- System policy is set so that the user has elevated privileges for installations
- Command AntiVirus has been advertised for all users
- Command AntiVirus has been assigned through Group Policy



Task name	Last results	Next scan on
Scan CD-Rom		
Scan Drive A		
Scan Drive B		
Scan Hard Drives		
Scan Network Drives		

Command AntiVirus Main Dialog Box

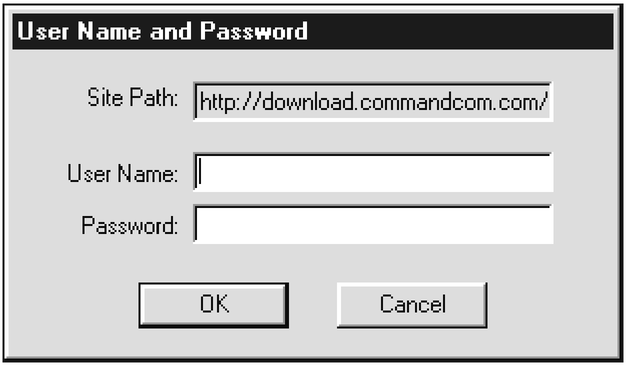
Downloads are attempted first from a list of Internet sites and then from the local sites according to the sort order of the sites in the site lists. The site at the top of the list is tried first. The site at the bottom is tried last.

By default, CSAV first tries to connect to the Command Software Systems web site. If this attempt is unsuccessful, it then tries to connect to the Command Software Systems FTP site.

To update the deffiles, follow these steps:

1. Click the **Update Deffiles** button. The system displays the **User Name and Password** dialog box.

NOTE: After you enter a **valid** user name and password for a specific **Site Path**, this dialog box does **not** display again as long as your user name and password for that site remain valid.


User Name and Password

Site Path: http://download.commandcom.com/

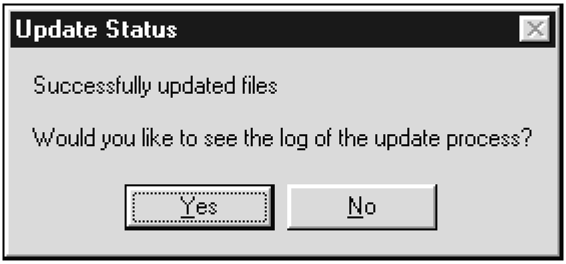
User Name:

Password:

User Name-Password Dialog Box

2. In the **User Name** text box, type your user name.
3. In the **Password** text box, type your password.
4. Click **OK**. CSAV tries to make the connection and downloads the definition files if new files are available.

   When the process is complete, the system displays the **Update Status** dialog box:


Update Status

Successfully updated files

Would you like to see the log of the update process?

Update Status Dialog Box

This dialog box displays the status of the download, for example:

```
Successfully updated files
```

It also gives you the option to view the details of the status in the log file.

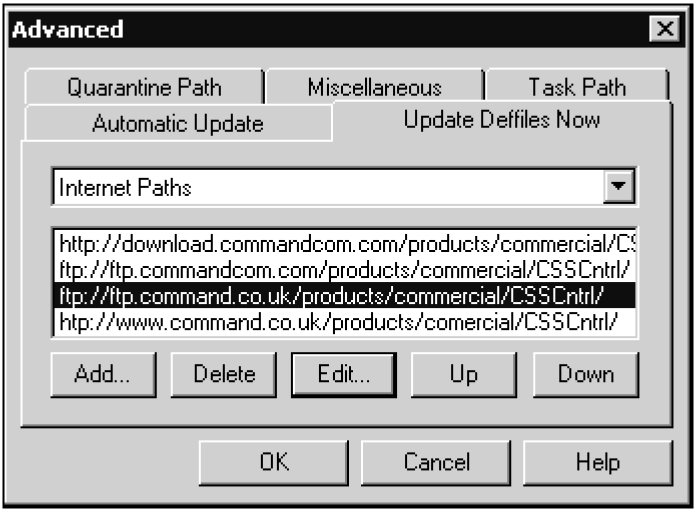
5. Click **No** to continue.

You can set which update sites the **Update Deffiles** button uses. Update sites can be local directories or on the Internet. Through the **Preferences**/**Advanced**/**Update Deffiles Now** dialog box, you can **Add**, **Remove**, and **Edit** the update sites. You can also change the order in which CSAV tries to connect to a site.

In Command AntiVirus for Windows NT/2000 and Command AntiVirus for Windows NT, you must be a member of the local Administrators group to perform these tasks.

To set the update sites, follow these steps:

1. On the menu bar, click **Preferences**. The system displays the drop-down menu.
2. Click **Advanced**. The system displays the **Advanced** dialog box.
3. Click the **Update Deffiles Now** tab. The system displays the **Update Deffiles Now** dialog box:



Internet Paths

http://download.commandcom.com/products/commercial/CS
ftp://ftp.commandcom.com/products/commercial/CSSCntrl/
ftp://ftp.command.co.uk/products/commercial/CSSCntrl/
http://www.command.co.uk/products/comercial/CSSCntrl/

Update Deffiles Now Dialog Box

4. Go to **Creating the Update Directory**.

Creating the Update Directory

Before you add a local directory to the **Directory Paths** site list, you **must** create an update directory structure.

NOTE: If you are using CSS Central, you do **not** need to create a separate update directory structure. Go to **Configuring Directory Sites** and add the directory path of your **staging** directory.

To create the update directory structure, follow these steps:

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

1. In a shared location on the network, create a unique parent directory, for example:

```
S:\UPDATES
```

2. Create the following subdirectories:

```
S:\UPDATES\NT351_S

S:\UPDATES\NT351_W

S:\UPDATES\NT40_S

S:\UPDATES\NT40_W

S:\UPDATES\WIN2000_S

S:\UPDATES\WIN2000_W

S:\UPDATES\WIN3X

S:\UPDATES\WIN95

S:\UPDATES\WIN32
```

3. Excluding the **WIN32** subdirectory, create the following product directory in each subdirectory listed in **Step 2**:

```
ANTIVIR\DEFFILES
```

For example, for Windows 95/98 Command AntiVirus files, create the following directory structure:

```
S:\UPDATES\WIN95\ANTIVIR\DEFFILES
```

4. In the **WIN32** subdirectory listed in **Step 2**, create the following product directories:

```
CSAV_LOTUSNOTES\DEFFILES

CSAV_EXCHANGE\DEFFILES
```

   For example, create the following directory structure:

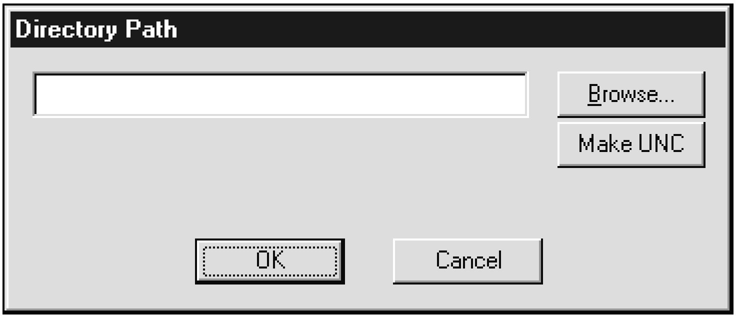
```
S:\UPDATES\WIN32\CSAV_LOTUSNOTES\DEFFILES

S:\UPDATES\WIN32\CSAV_EXCHANGE\DEFFILES
```

5. Download all of the files in the **DEFFILES** folder for each platform from our FTP or web site to the appropriate DEFFILES directory. For example, if the folder contains DEFFILES.EXE and FILES.LST, download both files.
6. Go to **Configuring Directory Sites** or **Configuring Internet Sites**.

Configuring Directory Sites

To **Add** a directory site, follow these steps:

1. In the **Update Deffiles Now** dialog box, click the down arrow and select **Directory Paths**.
2. Click **Add**. The system displays the **Directory Path** dialog box:



Directory Path Dialog Box

3. In the text box, type the path of the directory containing the CSAV virus definition files.

   To change a non-local directory path to a UNC path, click **Make UNC**.

NOTE: You can also use **Browse** to locate the directory. The system displays the **Open** dialog box. Select the directory and click **OK**.

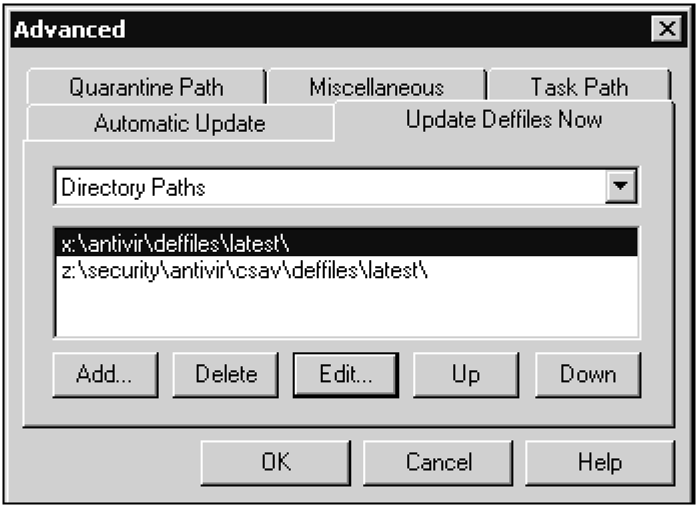
4. Click **OK**. You are returned to the **Update Deffiles Now** dialog box and the new path is added to the site list.
5. Click **OK** to finish.

To **Remove** a directory site, follow these steps:

1. In the **Update Deffiles Now** dialog box, click the down arrow and select **Directory Paths**. The system displays a list of directory sites.
2. Select a directory site from the list.
3. Click **Remove**. The site is removed from the list.
4. Click **OK** to finish.

To **Edit** a directory site, follow these steps:

1. In the **Update Deffiles Now** dialog box, click the down arrow and select **Directory Paths**. The system displays a list of directory sites that you have added:

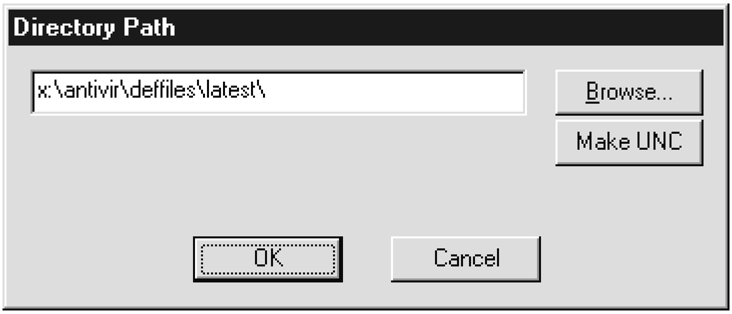


Directory Paths

x:\antivir\deffiles\latest\
z:\security\antivir\csav\deffiles\latest\

Directory Paths List Box

2. Select a directory site from the list.
3. Click **Edit**. The system displays the **Directory Path** dialog box:



x:\antivir\deffiles\latest\

Directory Path Dialog Box

4. Type the path of the directory containing the CSAV virus definition files in the text box.

   To change a non-local directory path to a UNC path, click **Make UNC**.

NOTE: You can also use **Browse** to locate the directory. The system displays the **Open** dialog box. Select the directory and click **OK**.

5. Click **OK**. You are returned to the **Update Deffiles Now** dialog box and the new path replaces the old path in the site list.
6. Click **OK** to finish.

To change the **sort order** of the sites, follow these steps:

1. In the **Update Deffiles Now** dialog box, click the down arrow and select **Directory Paths**. The system displays a list of directory sites.
2. Select a directory site from the list.
3. Click **Up** or **Down** to move site within the site list.
4. Click **OK** to finish.

NOTE: Downloads are attempted first from the Internet sites and then from the local sites. To make a local site a primary site, you must add the directory path to the Internet site list in the following format:

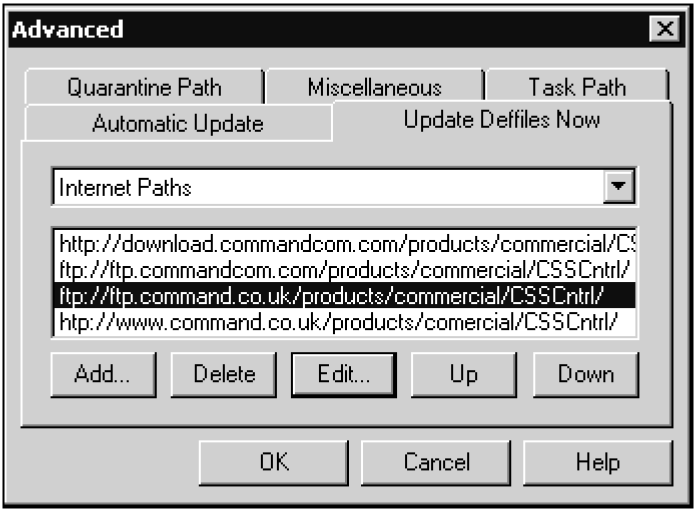
```
FILE://S:\UPDATE\WIN95\ANTIVIR\DEFFILES
```

Then, move the site to the top of the list.

Configuring Internet Sites

To **Add** an Internet site, follow these steps:

1. In the **Update Deffiles Now** dialog box, click the down arrow and select **Internet Paths**. The system displays a list of Internet sites.

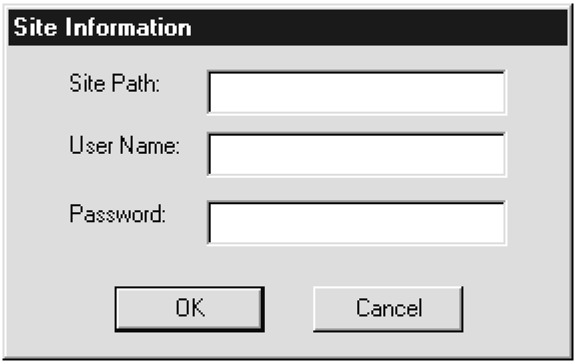


Internet Paths

http://download.commandcom.com/products/commercial/CS
ftp://ftp.commandcom.com/products/commercial/CSSCntrl/
ftp://ftp.command.co.uk/products/commercial/CSSCntrl/
http://www.command.co.uk/products/comercial/CSSCntrl/

Internet Paths List Box

2. Click **Add**. The system displays the **Site Information** dialog box:



Site Information Dialog Box

3. In the **Site Path** text box, type the address of the Internet update site.
4. In the **User Name** text box, type the user name needed to access the site.
5. In the **Password** text box, type the password for the user name that you entered in **Step 4**.
6. Click **OK**. You are returned to the **Update Deffiles Now** dialog box and the new path is added to the site list.
7. Click **OK** to finish.

To **Remove** an Internet site, follow these steps:

1. In the **Update Deffiles Now** dialog box, click the down arrow and select **Internet Paths**. The system displays a list of Internet sites.
2. Select an Internet site from the list.
3. Click **Remove**. The site is removed from the list.
4. Click **OK** to finish.

To **Edit** an Internet site, follow these steps:

1. In the **Update Deffiles Now** dialog box, click the down arrow and select **Internet Paths**. The system displays a list of Internet sites.
2. Select an Internet site from the list.
3. Click **Edit**. The system displays the **Site Information** dialog box.
4. In the **Site Path** text box, type the address of the Internet update site.
5. In the **User Name** text box, type the user name needed to access the site.
6. In the **Password** text box, type the password for the user name that you entered in **Step 5**.
7. Click **OK**. You are returned to the **Update Deffiles Now** dialog box and the new path replaces the old path in the site list.
8. Click **OK** to finish.

To change the **sort order** of the sites, follow these steps:

1. In the **Update Deffiles Now** dialog box, click the down arrow and select **Internet Paths**. The system displays a list of directory sites.
2. Select an Internet site from the list.
3. Click **Up** or **Down** to move the site within the site list.
4. Click **OK** to finish.

Disabling the Update Deffiles Button

If you do not want your users to be able to update definition files through the **Update Deffiles** button, you can disable it. When this function is disabled, the **Update Deffiles** button on the Command AntiVirus main dialog box is dimmed.

You can disable the **Update Deffiles** button by clearing the **Enable the Update Deffiles button** check box. You can also remove the **Update Deffiles Now** dialog box by clearing the **Show the Update Deffiles Now dialog box** check box. These check boxes are located in the **Specify CSAV Setup Running Options** dialog box of the Command AntiVirus Custom Installation Wizard. For more information, refer to **Customizing Your Installation Settings** located previously in this chapter.

CHANGING THE QUARANTINE FOLDER

In Command AntiVirus for Windows NT/2000 and Command AntiVirus for Windows NT, you must be a member of the local Administrators group to perform this task.

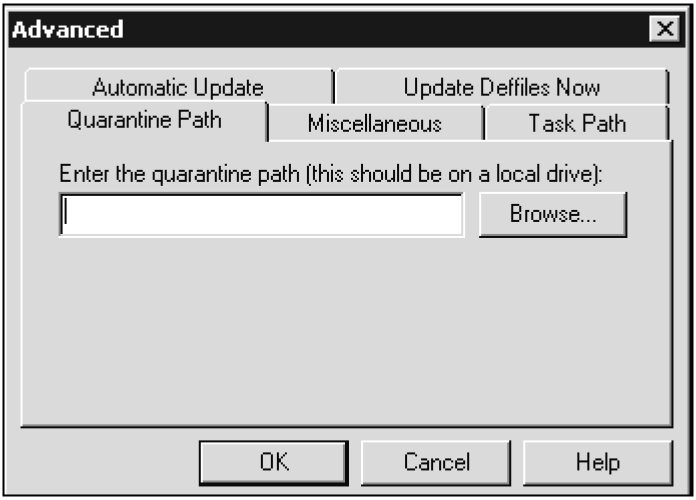
In the **Quarantine Path** dialog box, you can specify the path of a quarantine folder other than the default folder.

By default, Command AntiVirus creates a quarantine folder in the root directory of the system drive where Windows was installed. Entering a path to a different quarantine folder routes infected files to that folder rather than to the default folder.

If you set a path to a different quarantine folder, infected files are routed to that folder only if you select the **Quarantine** option in the **Preferences/Active Protection** dialog box and/or the scan task's **Properties** dialog box. Files that were located in a previously defined quarantine directory will **not** be moved or modified.

To change the default quarantine folder, follow these steps:

1. From the Command AntiVirus task bar, click **Preferences**. The system displays a drop-down menu.
2. Click **Advanced**. The system displays the **Advanced** dialog box.
3. Click the **Quarantine Path** tab. The system displays the **Quarantine Path** dialog box:



Enter the quarantine path (this should be on a local drive):

Quarantine Path Dialog Box

4. In the **Enter the quarantine path** text box, type the full path to the new quarantine folder.

NOTE: The folder should be located on a local drive. You can also use the **Browse** button to select the folder.

5. Click **OK**.

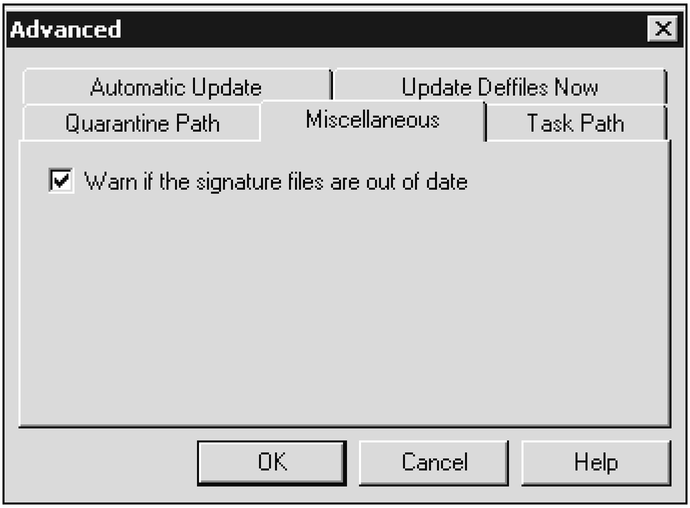
SETTING A DEFINITION FILES WARNING

In Command AntiVirus for Windows NT/2000 and Command AntiVirus for Windows NT, you must be a member of the local Administrators group to perform this task.

In the **Miscellaneous** dialog box, you can configure Command AntiVirus to provide a warning if its virus definition (signature) files are out-of-date. If you select this option, Command AntiVirus routinely checks the age of its definition files. When the definition files are out of date, the system displays a message advising the user that the signature files should be updated.

To receive a warning when the virus definition files are out-of-date, follow these steps:

1. From the Command AntiVirus task bar, click **Preferences.** The system displays a drop-down menu.
2. Click **Advanced**. The system displays the **Advanced** dialog box.
3. Click the **Miscellaneous** tab. The system displays the **Miscellaneous** dialog box:



☑ Warn if the signature files are out of date

Miscellaneous Dialog Box

4. Select the **Warn if the signature files are out of date** check box
5. Click **OK**.

CHANGING THE SYSTEM SCAN TASK FOLDER

In Command AntiVirus for Windows NT/2000 and Command AntiVirus for Windows NT, you must be a member of the local Administrators group to perform this task.

In the **Task Path** dialog box, you can specify the path of a folder other than the default folder that contains the Command AntiVirus system scan task files.

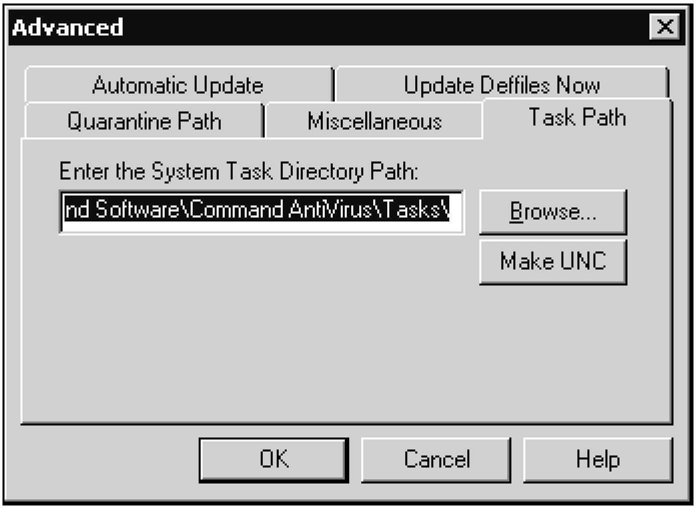
By default, the operating system stores the system scan tasks in a predetermined folder on the hard drive. Scan task files always use an .FPT extension.

As a network administrator, you may want to create global scan task files configured to your specifications that can be accessed by all users. For example, suppose all users have their own copy of Command AntiVirus installed on their local computer. However, you do not want to go to each workstation to add or update these scan tasks. The solution is to create the task files and store them in a central location on the network.

The **Task Paths** option can also be helpful if users run Command AntiVirus from the network but want to have their own individual scanning tasks. In this case, the tasks can be located on the local workstation and the **Task Paths** option can be used to point to the local drive.

To change the default Command AntiVirus system scan task folder, follow these steps:

1. From the Command AntiVirus task bar, click **Preferences**. The system displays a drop-down menu.
2. Click **Advanced**. The system displays the **Advanced** dialog box.
3. Click the **Task Path** tab. The system displays the **Task Path** dialog box:



Enter the System Task Directory Path: nd Software\Command AntiVirus\Tasks\

Task Path Dialog Box

4. In the **Enter the System Task Directory Path** text box, type the full path to the new folder.

NOTE: You can also use the **Browse** button to select the folder.

5. Click **OK**.

The scan tasks in the new location will be displayed in the **Command AntiVirus Main** dialog box.

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 for DOS 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 /TODAY option writes a very small data file that must remain on the local drive (or on any drive to which the user has “write” access).

7

CSS CENTRAL

CSS Central is an administrative tool for distributing, updating and modifying Command AntiVirus from one location.

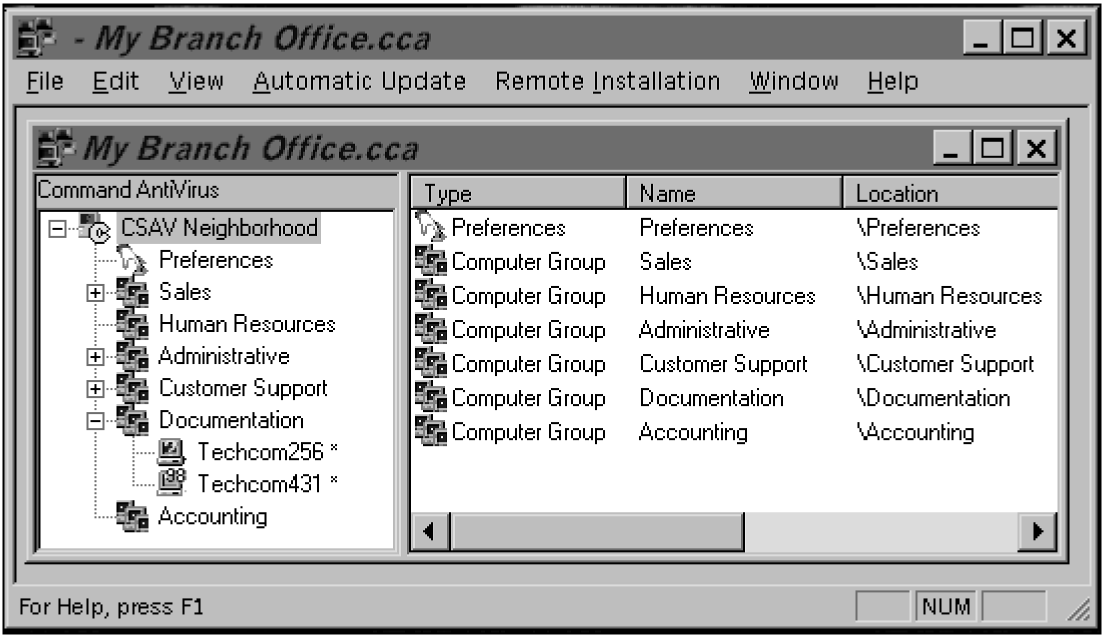
CSS Central can be used to administer the following:

- Command AntiVirus V. 4.5 and later for Windows® 95/98/Me
- Command AntiVirus V. 4.5 and later for Windows NT® 3.51/4.00 Workstation
- Command AntiVirus V. 4.5 and later for Windows NT®3.51/4.00 Server
- Command AntiVirus V. 4.59 and later for Windows NT®/2000 Workstation
- Command AntiVirus V. 4.60 and later for Windows NT®/2000 Server

With CSS Central, system administrators can:

- Configure Command AntiVirus protection for individual computers or computer groups. For example, you can change your **Preferences** settings and create and modify individual scanning tasks.
- Schedule CSS Central to download the latest Command AntiVirus files.
- Deploy and update Command AntiVirus for Windows 3x, 95/98/Me, NT Workstation and Server, and 2000 Workstation and Server to multiple computers on your network. Deployment can be performed through a NetWare® login script or by having mail recipients execute a special e-mail attachment.

Once you have created a database, the database window has two panes. The left pane displays a tree view that always contains a graphical display of the computers and computer groups that are managed under CSS Central. The root of the tree view is an object called **CSAV Neighborhood**. The right pane reflects the details of the currently selected item in the tree view.



Type	Name	Location
Preferences	Preferences	\Preferences
Computer Group	Sales	\Sales
Computer Group	Human Resources	\Human Resources
Computer Group	Administrative	\Administrative
Computer Group	Customer Support	\Customer Support
Computer Group	Documentation	\Documentation
Computer Group	Accounting	\Accounting

CSAV Neighborhood

Administrators can create their own groups and add computers to the **CSAV Neighborhood** by **dragging and dropping** in the tree view. A computer group can contain computers or even other computer groups. However, an individual computer can reside in only **<u>one</u>** 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.

SYSTEM REQUIREMENTS

CSS Central can be run on Microsoft® Windows 2000 server and workstation, Windows NT server and workstation version 4.0 and above, and on Windows 95, Windows 98, and Windows Me.

NOTE: You cannot install CSS Central on systems running versions of Windows NT prior to 4.0. However, servers and workstations running Windows NT 3.51 and Windows 3.11 can be administered.

Windows 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). As CSS Central operates primarily on outbound connections, this should not be an issue if it is run from a workstation. However, depending upon your configuration, CSS Central may experience problems connecting to NT workstations if the limit is reached.

For scheduled downloads to occur, the Windows Task Scheduler **must** be installed. This service comes with Microsoft Internet Explorer 4.0 and higher. As Windows 98, Windows Me, and Windows 2000 come with Internet Explorer, these versions also come with the Task Scheduler preinstalled. For Windows 95 and Windows NT 4.0, you must install Internet Explorer 4.0 or higher separately. If you did not install the Task Scheduler when you installed Internet Explorer 4.0, you can download a component update from the Microsoft site at:

http://www.microsoft.com/windows/ie/ie401/download/sp2/x86/en/download/setup.htm

CSS Central supports TCP/IP and IPX/SPX networking 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.

To maintain and change the CSAV settings on a remote computer, the communications subsystem installed with CSAV 4.5x or higher must be running on that computer.

In addition, to administer CSAV on your network, you **must** be able to view remote computers from Network Neighborhood. To view remote computers in Windows 95/98/Me, you **must** have file and print sharing enabled on the computers.

INSTALLATION

The following instructions will help you to install CSS Central quickly and easily. The default installation installs all of the required components. However, during the installation you will have the opportunity to select the components that you want to install.

We suggest that you read through these instructions prior to installing the product. This will allow you to better anticipate any choices that you may need to make during the installation process.

INSTALLING

NOTE: Before running the installation program, we strongly recommend that you exit all Windows programs.

NOTE: As the CSS Central files install to the **Program Files** folder, you **must** have appropriate privileges to install CSS Central on Microsoft Windows NT and Windows 2000 on NTFS drives.

NOTE: As the CSSFTP.INI file is stored in the **All Users**/**Application Data** profile folder, you must have administrative privileges to install and customize this file on Microsoft Windows NT and Windows 2000.

NOTE: For machines that do not have the Windows Installer, a **SETUP.EXE** is provided. It installs the Windows Installer and then launches the **CCENTRAL.MSI**.

For Windows NT, you **must** have administrative privileges to install the Windows Installer.

After installing the Windows Installer, the user may need to restart the computer. After, the computer restarts, Setup continues.

NOTE: The default installation now includes only the IP components subfeature. If you are using SPX protocol, you need to customize the installation. As we recommend that you select only **one** Communication System subfeature, cancel the IP components subfeature selection and select the SPX components subfeature.

To install CSS Central, follow these steps:

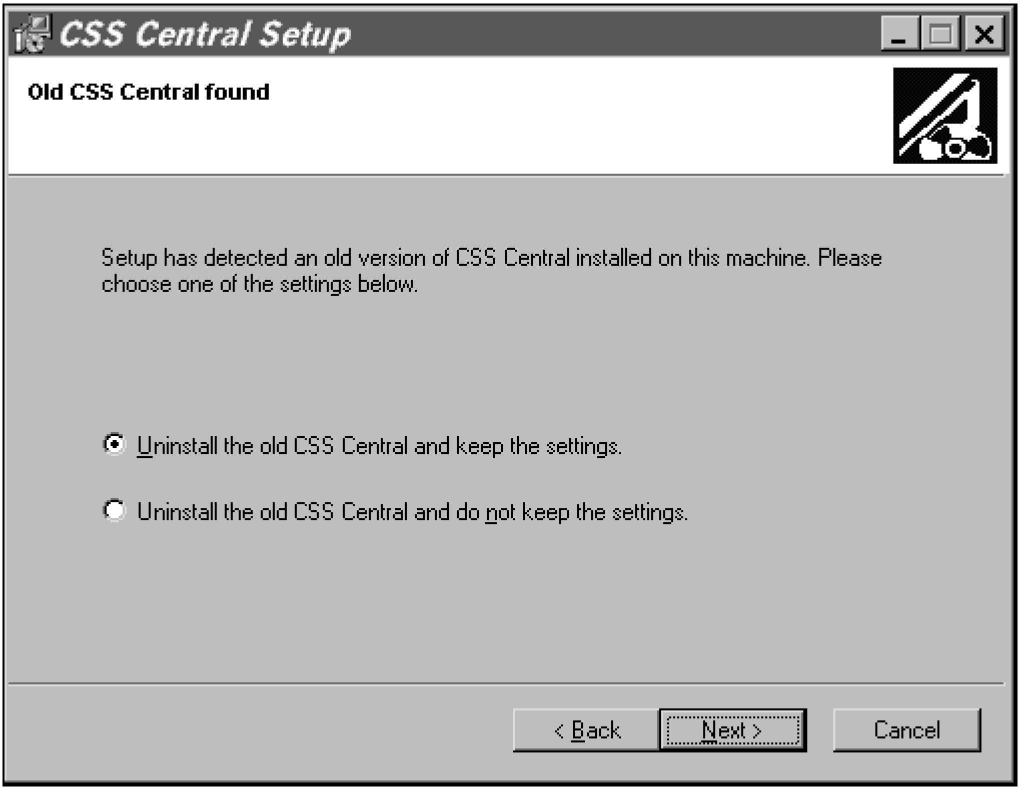
1. Insert the CD-ROM.
2. Click the **Start** button on the Windows task bar.
3. Click **Run**.
4. Click **Browse** to search the CD for the **CCENTRAL** folder.
5. Open that folder.
6. In the **File of type** drop-down, select **All Files**.
7. To run the setup program in **Windows 2000 and ME:** Double-click **CCENTRAL.MSI**.

   To run the setup program in **Windows 95/98** and **Windows NT:** Double-click **SETUP.EXE**.

   The system returns to the **Run** dialog box.
8. Click **OK**. The system displays the **Welcome** dialog box.
9. Click **Next**. The system displays the **License Agreement**.
10. To accept the license agreement, select **I accept the License Agreement** and click **Next**.

    If you do **not** have an old version of CSS Central installed, go to **Step 11**.

    If you have an old version of CSS Central installed, the system displays the **Old CSS Central Found** dialog box:



CSS Central Setup

Old CSS Central found

Setup has detected an old version of CSS Central installed on this machine. Please choose one of the settings below.

● Uninstall the old CSS Central and keep the settings.

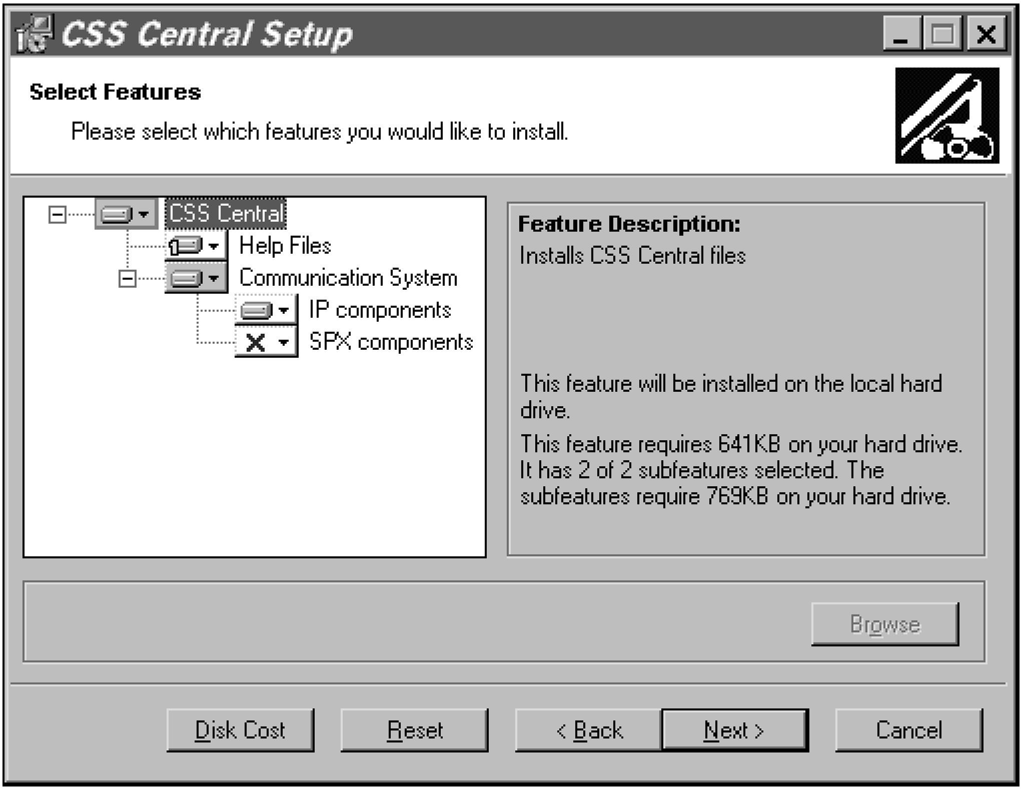
○ Uninstall the old CSS Central and do not keep the settings.

Old CSS Central Found Dialog Box

In this dialog box, select **one** of the following options, and then click **Next**:

- Uninstall the old CSS Central and keep your old settings
- Uninstall the old CSS Central and do **not** keep your old settings

11. The system displays the **Select Features** dialog box:



CSS Central Setup

Select Features

Please select which features you would like to install.

- CSS Central
  - Help Files
  - Communication System
    - IP components
    - ☒ SPX components

Feature Description:
Installs CSS Central files

This feature will be installed on the local hard drive.

This feature requires 641KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 769KB on your hard drive.

Select Features Dialog Box

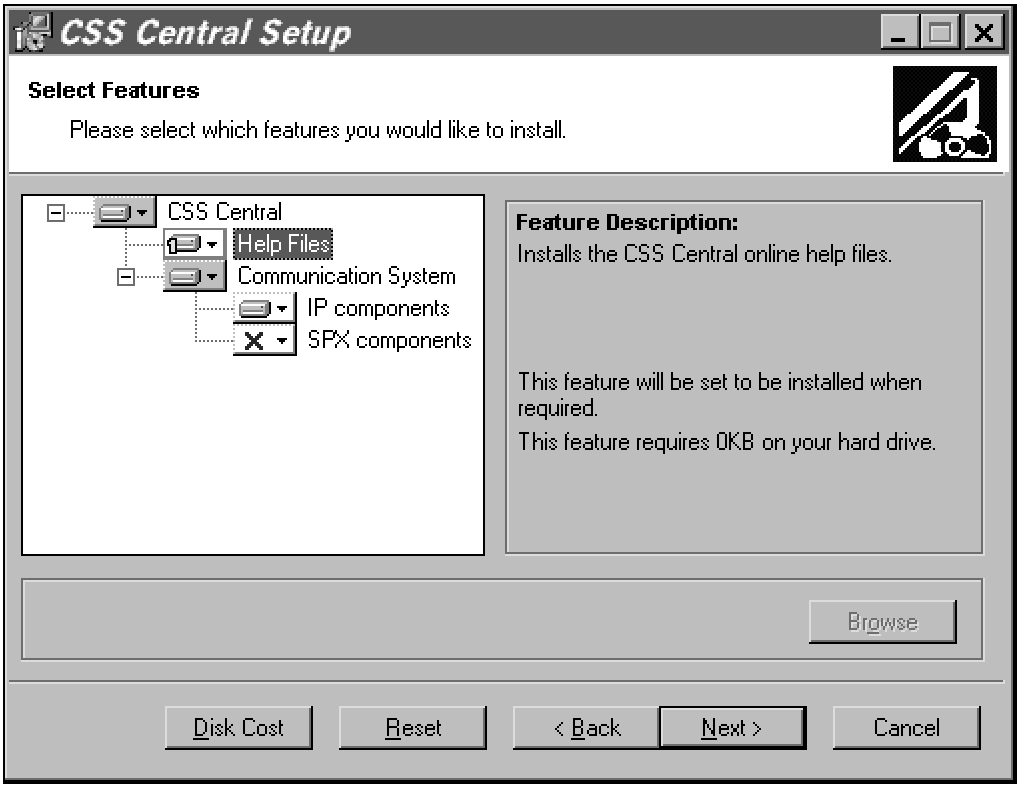
Select **one** of the following:

- If you want to accept the default selections, go to **Step 12**.

NOTE: The default installation includes only the **IP components** subfeature. If you are using **SPX** protocol, you need to customize the installation. As we recommend that you select only **one** Communication System subfeature, cancel the **IP components** subfeature selection, and select the **SPX components** subfeature.

- If you want to customize the installation, select the features and subfeatures that you want to install.

You can view the description of each feature and subfeature by clicking its name. For example, click **Help Files**:



CSS Central Setup

Select Features

Please select which features you would like to install.

- CSS Central
  - Help Files
  - Communication System
    - IP components
    - SPX components

Feature Description:

Installs the CSS Central online help files.

This feature will be set to be installed when required.

This feature requires 0KB on your hard drive.

Select Features Dialog Box - Help Files Description

CSS Central – installs all of the CSS Central files. This feature is installed by default.

NOTE: This feature installs only the **IP components** subfeature by default. If you are using **SPX** protocol, you need to customize the installation. As we recommend that you select only **<u>one</u>** Communication System subfeature, cancel the **IP components** subfeature selection, and select the **SPX components** subfeature.

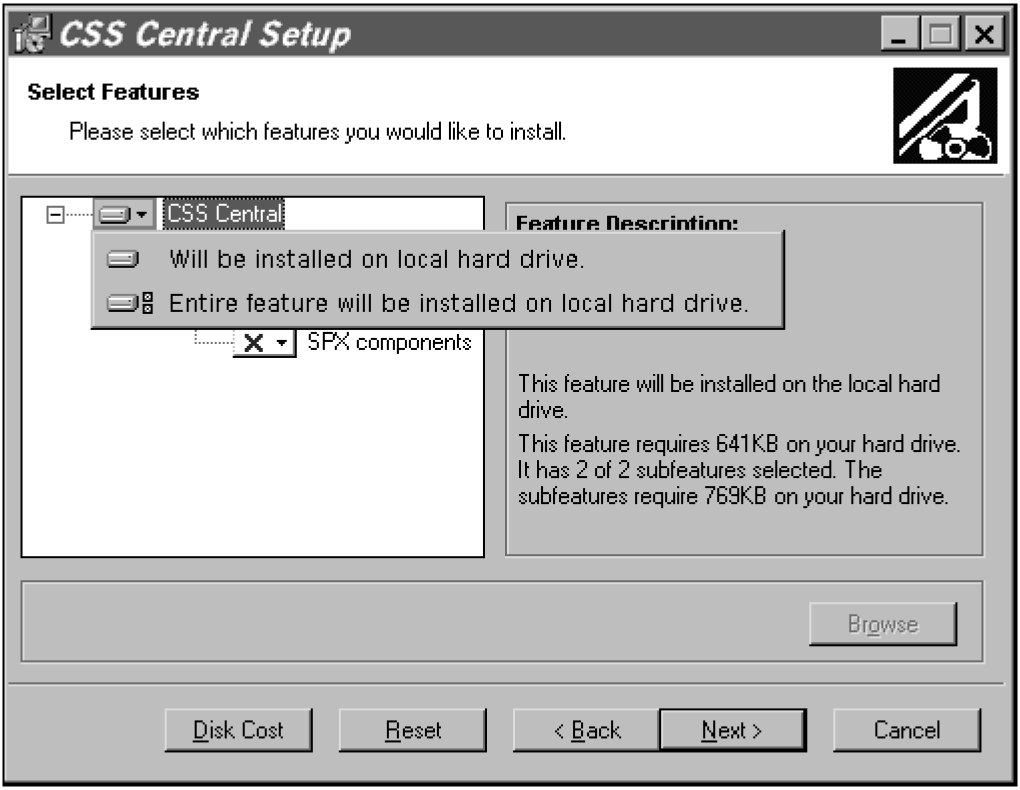
The CSS Central feature contains the following subfeatures:

- **Help Files** – installs the CSS Central online help files. By default, this subfeature is installed the first time it is accessed.
- **Communication System** – installs the files that are required by CSS Central to remotely administer computers that are running Command AntiVirus. This subfeature is installed by default.

  The Communication System contains the following subfeatures. If you are using only one protocol, we recommend that you select only the subfeature for that protocol.

  - **IP components** – installs the IP port location for the communication subsystem that is used by CSS Central for managing Command AntiVirus. The **IP components** subfeature is required to read or write configurations or broadcast updates. This subfeature is installed by default.
  - **SPX components** – installs the SPX port location for the communication subsystem that is used by CSS Central for managing Command AntiVirus. The **SPX components** subfeature is required to read or write configurations or broadcast updates. This subfeature is **<u>not</u>** installed by default.

To the left of each feature and subfeature is an icon that represents the present installation state. To view the explanation of each icon or to select a different installation state, click the down arrow ▾ to the right of the icon. The system displays a drop-down menu:



CSS Central Setup
Select Features
Please select which features you would like to install.
CSS Central
Will be installed on local hard drive.
Entire feature will be installed on local hard drive.
SPX components
Feature Description:
Browse
Disk Cost
Reset
< Back
Next >
Cancel

This feature will be installed on the local hard drive.

This feature requires 641KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 769KB on your hard drive.

Drop-Down Menu

NOTE: When the installation state of a subfeature is different from the state of the feature, the icon of the feature has a gray background.

Depending on the feature or subfeature that you select, the drop-down menu contains all or some of the following items:

Will be installed on local hard drive – installs the selected feature or subfeature on the local hard drive. If you select a subfeature, this option also installs the parent feature. For example, if you select to install the online **Help Files**, the **CSS Central** feature is also installed.

Entire feature will be installed on local hard drive – installs the selected feature and all of its subfeatures on the local hard drive. For example, if you select the **CSS Central**, the **Help Files** and the **IP components** are also installed.

If you select a subfeature, this option installs the parent feature and the selected subfeature. For example, if you select to install **Communication System, CSS Central** is also installed.

Feature will be installed when required – installs the selected feature the first time it is accessed. For example, if you select this option for the online **Help Files, Help** is installed only the first time it is used.

NOTE: You **must** have Windows Desktop Update installed to be able to use the **Feature will be installed when required** installation state. Active Desktop does not have to be enabled.

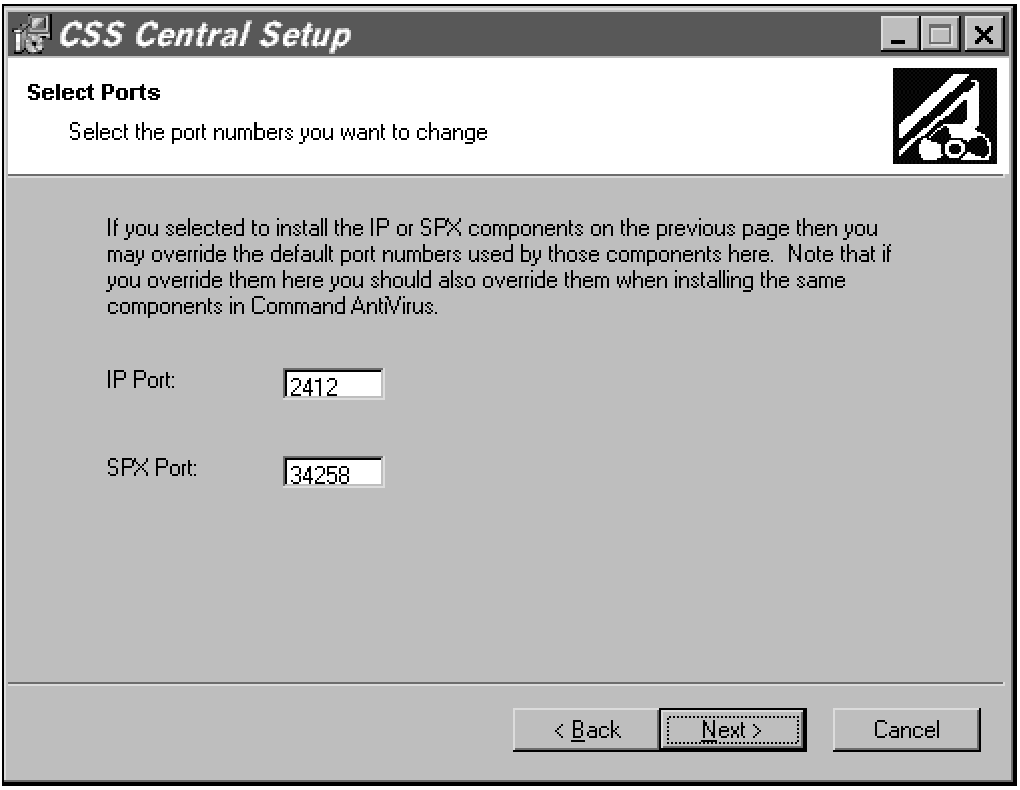
Entire feature will be unavailable – does **not** install the selected feature or any of its subfeatures.

To change the installation state for a selected feature or subfeature, click the appropriate icon. The program returns to the **Select Features** dialog box which now shows the installation state icon that you selected.

NOTE: To reset the features and subfeatures to the default selections, click **Reset**. To view details of the amount of disk space that a feature or subfeature requires on the hard drive, click **Disk Cost**.

12. Click **Next**. The system displays the **Select Ports** dialog box:

NOTE: If you did **not** select to install either the **IP component** or the **SPX component**, click **Next**, and go to **Step 14**.



CSS Central Setup

Select Ports

Select the port numbers you want to change

If you selected to install the IP or SPX components on the previous page then you may override the default port numbers used by those components here. Note that if you override them here you should also override them when installing the same components in Command AntiVirus.

IP Port: 2412

SPX Port: 34258

Select Ports Dialog Box

This dialog box allows you to change the default **IP Port** and **SPX Port** location numbers.

NOTE: If you change the default port numbers in this dialog box, you should also change them when you install the same components in Command AntiVirus.

13. Type the new number in the appropriate text box and click **Next**.

NOTE: The installation program accepts only decimal values.

14. The system displays the **Updating System** dialog box. Please wait while the program copies the CSS Central files to your system.

NOTE: If you selected to uninstall an old version of CSS Central, the system first starts the uninstall and displays the **Remove Programs From Your Computer** dialog box. When the uninstall is complete, click **OK** to exit this dialog box.

NOTE: You can click **Cancel**, **Exit Setup** and then **OK** to cancel the installation and exit the setup program.

When the copying is complete, the system displays a dialog box informing you that CSS Central has been successfully installed.

15. Click **Finish** to exit.

When the installation is complete, go to **Setting Up CSS Central** located later in this chapter.

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 that always contains a graphical display of the computers and computer groups that are managed under CSS Central. The root of the tree view is an object called **CSAV Neighborhood**.

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** that is applied to all computers. Every descendant (**child**) of a computer group **inherits** (from the **parent)** that group's configuration. You can change this configuration for a specific computer or group of computers by creating a child object (a task or preference) with its own settings. For example, if you want all of the computers except one to be identical, you can create a task or preference that only applies to that computer. 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 effects the appearance of the list view displayed in the right pane.

DOUBLE-CLICK

When you double-click a computer or group icon in the tree view, a new window opens with a list view the same as 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 95/98/ME, a user 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.

For example, 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**.

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.

Automatic Update Menu

The **Automatic Update** menu allows you to configure the download sites, set Proxy Server settings, 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 message 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 from the **automatic update directory**.

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 computer group 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.

Automatic Update Menu

In addition to allowing you to configure the download sites, set Proxy Server settings,   download the latest version of Command AntiVirus, and automatically distribute the updates, this **Automatic Update Menu** allows you to send notification messages that the updates are available.

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 message 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 from the **automatic update directory**.

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.

SETTING UP CSS CENTRAL

Setting up CSS Central for the first time includes the following tasks. For CSS Central to work properly, you **must** complete these tasks in the order that they are discussed.

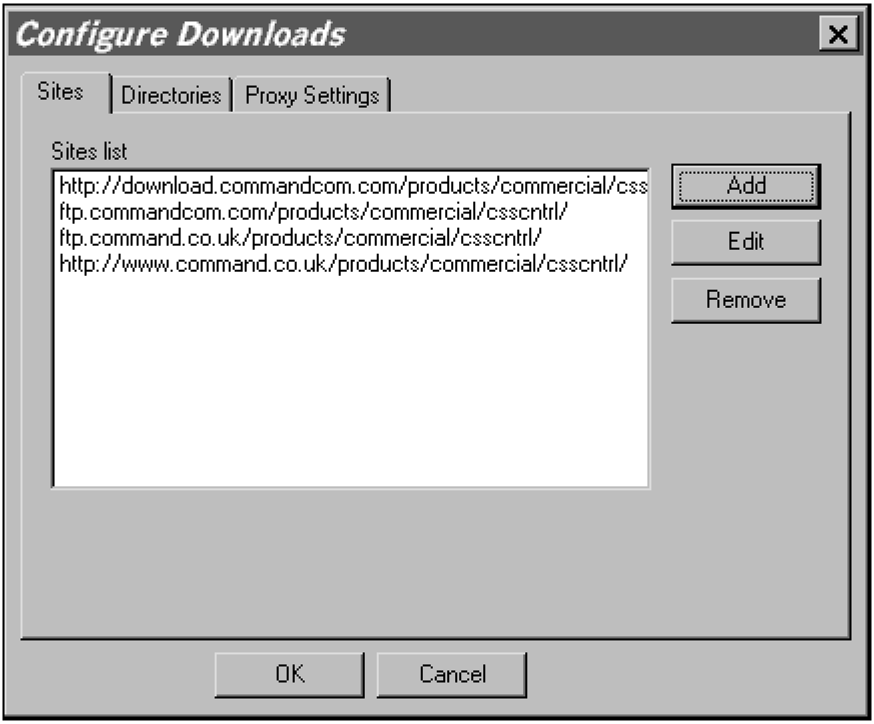
- Configuring the download process
- Downloading the Command AntiVirus files to the **staging directory**
- Deploying the files to the **automatic update directory**
- Verifying the deployment status of files
- Editing the SETUP.INI file
- Rolling out Command AntiVirus across your network
- Creating a CSS Central Database
- Administering Command AntiVirus on your network

CONFIGURING THE DOWNLOAD PROCESS

Through the **Configure Downloads** dialog box, you can specify whether you want to download the latest Command AntiVirus (CSAV) updates from an Internet site or a local directory. You can also specify your **staging directory, automatic update directory**, and **proxy server settings.**

To access the **Configure Downloads** dialog box, follow these steps:

1. On the CSS Central menu bar, click **Automatic Update**. The system displays the drop-down menu.
2. Click **Configure Downloads**. The system displays the **Configure Downloads** dialog box:



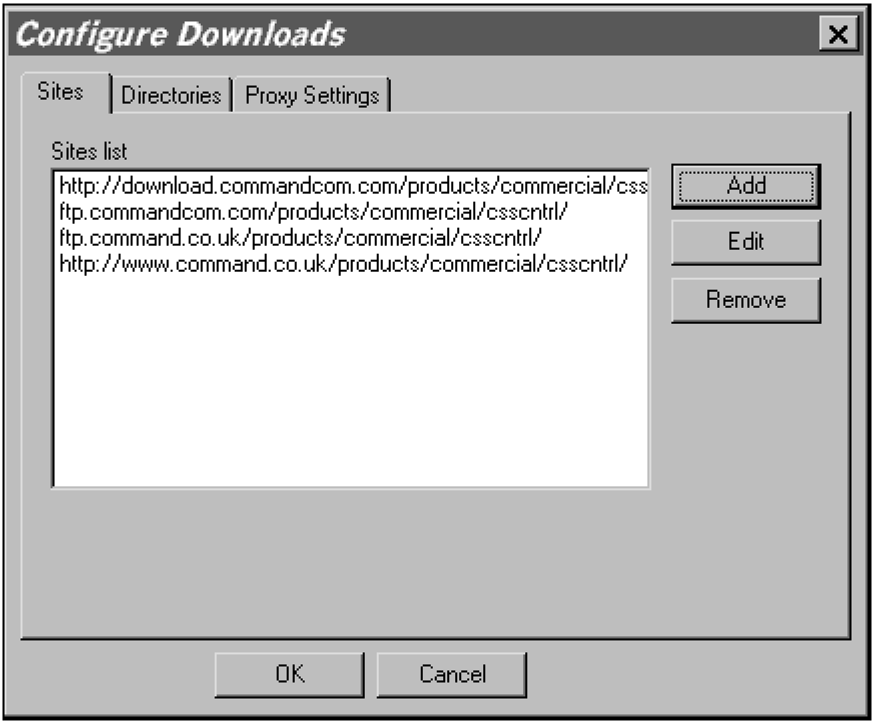
```
http://download.commandcom.com/products/commercial/css
ftp.commandcom.com/products/commercial/csscntrl/
ftp.command.co.uk/products/commercial/csscntrl/
http://www.command.co.uk/products/commercial/csscntrl/
```

Configure Downloads Dialog Box

The **Configure Downloads** dialog box contains three dialog boxes: **Sites**, **Directories**, and **Proxy Settings**. To access a specific dialog box, just click the appropriate tab.

Configuring the Download Sites

Downloads are attempted from the list of sites specified in the **Sites** dialog box:



http://download.commandcom.com/products/commercial/css
ftp.commandcom.com/products/commercial/csscntrl/
ftp.command.co.uk/products/commercial/csscntrl/
http://www.command.co.uk/products/commercial/csscntrl/

Configure Downloads - Sites Dialog Box

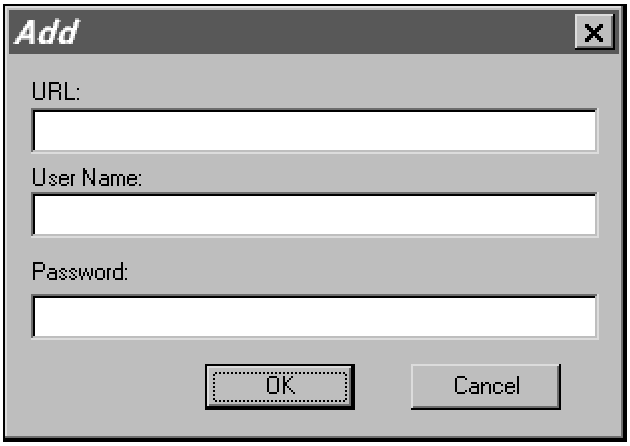
The site at the top of the list is tried first. The site at the bottom is tried last.

By default, CSS Central first tries to connect to the Command Software Systems web site. If this attempt is unsuccessful, it then tries to connect to the Command Software Systems FTP site.

From this dialog box, you can **Add**, **Edit**, or **Remove** a site from the **Sites list**.

To **Add** a site, follow these steps:

1. In the **Sites** dialog box, click **Add.** The system displays the **Add** dialog box:

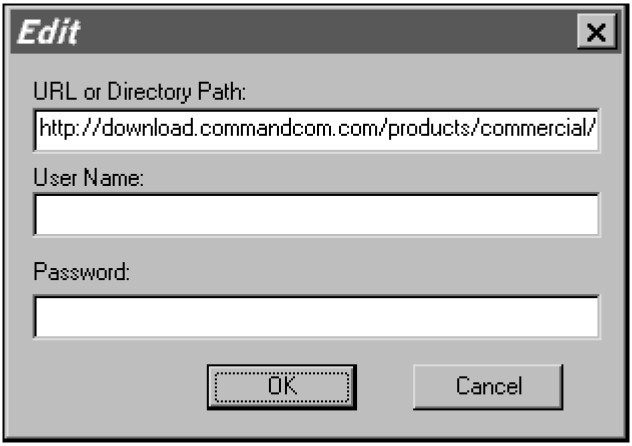


Add Dialog Box

2. In the **URL** text box, type the web URL that you want to add.
3. In the **User Name** text box, type your user name for the URL that you specified.
4. In the **Password** text box, type your password.
5. Click **OK**. The system returns to the **Sites** dialog box and the new site is added to the bottom of the **Sites list**.
6. Click **OK** to exit the dialog box.

To **Edit** a site, follow these steps:

1. In the **Sites** dialog box, select a site from the **Sites list**, and then click **Edit.** The system displays the **Edit** dialog box:



URL or Directory Path: http://download.commandcom.com/products/commercial/

Edit Dialog Box

2. In the **URL or Directory Path** text box, edit the web URL or local directory path that you want to change.
3. In the **User Name** text box, type your user name for the URL or directory path that you specified**.**
4. In the **Password** text box, type your password.
5. Click **OK**. The system returns to the **Sites** dialog box and the site is the **Sites list**.
6. Click **OK** to exit the dialog box.

To **Remove** a site, follow these steps:

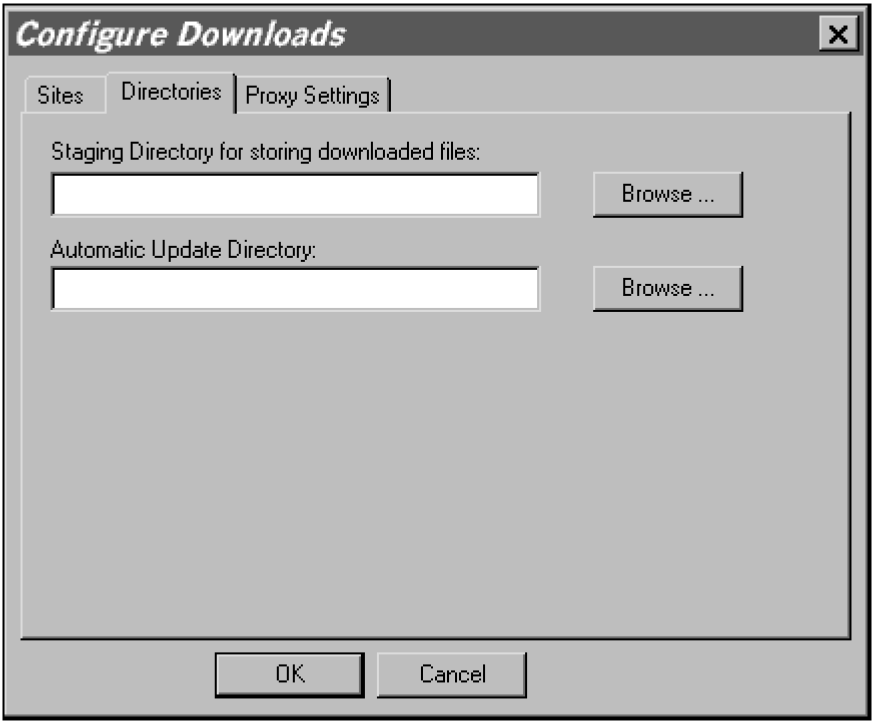
1. In the **Sites** dialog box, select a site from the **Sites list**, and then click **Remove**. The site is removed from the list.

2. Click **OK** to exit the dialog box.

Specifying the Staging and Automatic Update Directories

CSS Central keeps the downloaded updates in a **staging directory.** Once the updates are downloaded into the **staging directory**, they are deployed to the CSS Central **automatic update directory.** CSS Central can then use those files to update your network's computers with the latest Command AntiVirus protection.

You can specify the **staging directory** and the **automatic update directory** in the **Directories dialog**:



Configure Downloads - Directories Dialog Box

To specify the **staging directory** and the **automatic update directory**, follow these steps:

1. In the **Staging Directory for storing downloaded files** text box, enter the path to a temporary (**staging**) directory that will temporarily hold the downloaded Command AntiVirus files, for example:

```
C:\STAGING
```

NOTE: You can use the **Browse** button to select the directory.

Do **not** manually add or remove anything in this directory. CSS Central uses this directory for its own file management.

2. In the **Automatic Update Directory** text box, enter the path to a shared directory. This is necessary for rolling out CSAV updates to remote computers.

   For example, if you have shared drive and you are using APS as the share name for all of the software for your users, add a CSAV directory under APS to use as the **automatic update directory**:

```
M:\APS\CSAV
```

NOTE: We recommend that you use 8-character file names. Universal Naming Convention **(**UNC**)** paths can be substituted for mapped drives:

```
\\MAINSERVER\APS\CSAV
```

3. Click **OK**. The system displays a dialog box asking you if you want to create the directory that you specified for the **staging directory**.

4. Click **Yes**. If you created the directory on a remote path, you may experience a slight delay as CSS Central tries to access the directory.

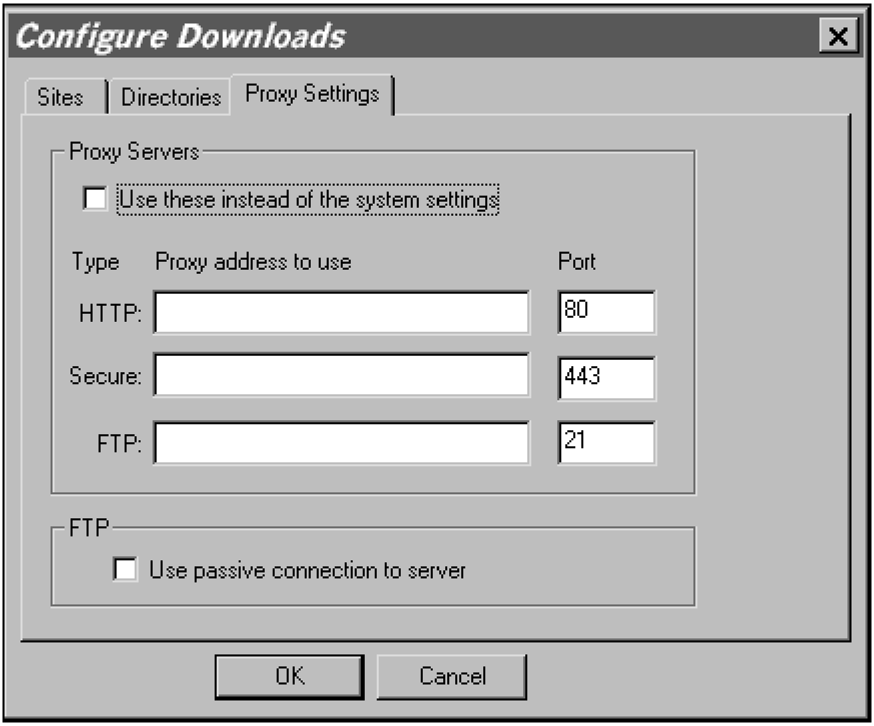
   The system displays a dialog box asking you if you want to create the directory that you specified for the **automatic update directory.**

5. Click **Yes**. If you created the directory on a remote path, you may experience a slight delay as CSS Central tries to access the directory.

   The system returns to the **CSAV Neighborhood**.

Specifying Proxy Server Settings

The **Proxy Settings** dialog box allows you to override the Windows default settings to download Command AntiVirus through a proxy server. You can specify an address and port number for **HTTP**, **HTTP Secure**, and **FTP** requests. For **FTP** requests, you can also select to use passive connection to the server:



Proxy Servers

□ Use these instead of the system settings

Type	Proxy address to use	Port
HTTP:		80
Secure:		443
FTP:		21

FTP

□ Use passive connection to server

Configure Downloads - Proxy Settings Dialog Box

To specify your proxy server settings, follow these steps:

1. In the **Proxy Settings** dialog box, under **Proxy Servers**, select the **Use these instead of the system settings check box**.
2. In the **HTTP** text box, type the address of the proxy server that you want to use for **HTTP** requests such as MYPROXYSRV.
3. In the **Port** text box, type the port number for that address.
4. In the **Secure text** box, type the address of the proxy server that you want to use for secure HTTP requests, for example, requests to a lock box on a secure site.
5. In the **FTP** text box, type the address of the proxy server that you want to use for FTP requests such as MYPROXYSRV.
6. In the **Port** text box, type the port number for that address.

NOTE: The default connection to the server for FTP requests is **active**. If you need to use FTP through a firewall, you can change this connection to **passive** by selecting the **Use passive connection to server** check box under **FTP**.

7. Click **OK** to save the settings. The system returns to the **CSAV Neighborhood**.
8. If you are setting up CSS Central for the first time, go to **Downloading the Command AntiVirus Files**.

DOWNLOADING THE COMMAND ANTIVIRUS FILES

The options in the **Schedule downloads** dialog box allow you to tell CSS Central which update files it should download from the Command Software Systems web site or FTP site. This download can be performed automatically (scheduled) or manually (immediate).

The **Scheduled downloads** dialog box contains two dialog boxes: **Schedule** and **Immediate**. To access a specific dialog box, just click the appropriate tab.

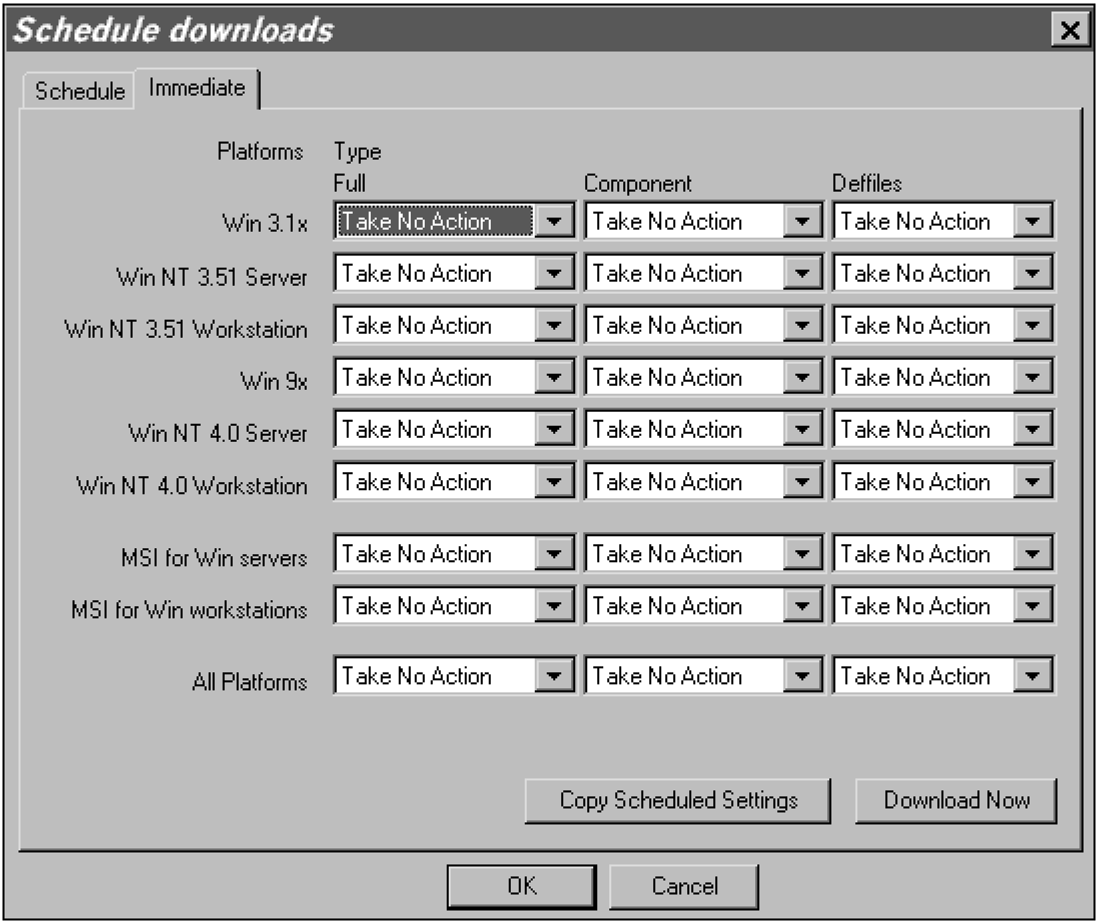
Performing a Manual Download

The **Immediate** dialog box allows you to download Command AntiVirus files on-demand. You do not have to wait for a scheduled download to occur. This feature allows you to test the settings that you want to select for the scheduled downloads, or to download a specific platform immediately.

NOTE: If you are setting up CSS Central for the first time or are changing any of the settings that you have previously selected, we recommend that you perform a manual (immediate) download of the Command AntiVirus files to test your settings.

To download the Command AntiVirus files into the CSS Central **staging directory** manually and automatically deploy them to the **automatic update directory**, follow these steps:

1. On the CSS Central menu bar, click **Automatic Update**. The system displays the drop-down menu.
2. Click **Schedule downloads**. The system displays the **Schedule downloads** dialog box.
3. Click the **Immediate** tab. The system displays the **Immediate** dialog box:



Platforms	Type Full	Component	Deffiles
Win 3.1x	Take No Action	Take No Action	Take No Action
Win NT 3.51 Server	Take No Action	Take No Action	Take No Action
Win NT 3.51 Workstation	Take No Action	Take No Action	Take No Action
Win 9x	Take No Action	Take No Action	Take No Action
Win NT 4.0 Server	Take No Action	Take No Action	Take No Action
Win NT 4.0 Workstation	Take No Action	Take No Action	Take No Action
MSI for Win servers	Take No Action	Take No Action	Take No Action
MSI for Win workstations	Take No Action	Take No Action	Take No Action
All Platforms	Take No Action	Take No Action	Take No Action

Schedule Downloads - Immediate Dialog Box

4. Under **Platforms Type**, locate the platform that you want to download.

NOTE: If you have already scheduled your downloads, you can copy the platforms and the settings that you selected in the **Schedule** dialog box, by clicking the **Copy Scheduled Settings** button. Then go to **Step 8**.

5. In the **Full** list, click the drop-down arrow, and select **Download/Deploy**.

NOTE: If you only want to download the files to the **staging directory**, select **Download**. You can deploy the files to the automatic update directory at a later time. For more information, refer to **Deploying the Downloaded Files to the Automatic Update Directory**.

6. In the **Component** list, click the drop-down arrow, and select **Download/ Deploy**.
7. In the **Deffiles** list, click the drop-down arrow, and select **Download/Deploy**.
8. To start the download, click the **Download Now** button.

NOTE: If you did not enter a valid user name and password in the **Sites** dialog box, the system displays an **Invalid User Name or Password** dialog box. Enter a valid user name and password. The information is saved for future connections.

9. When the download is complete, click **OK**.

NOTE: If the download fails, the system displays the **Failed to download updated files** dialog box with an option to view the update log.

10. Repeat **Steps 4** through **9** for any other platforms that you need to test or install on your network computers.
11. Click **OK** to exit.
12. If you are setting up CSS Central for the first time, go to **Configuring Your Scheduled Downloads**.

Configuring Your Scheduled Downloads

NOTE: For scheduled downloads to occur, the Windows Task Scheduler **must** be installed. This service comes with Microsoft Internet Explorer 4.0 and higher.

As Windows 98, Windows Me, and Windows 2000 come with Internet Explorer, these versions also come with the Task Scheduler preinstalled.

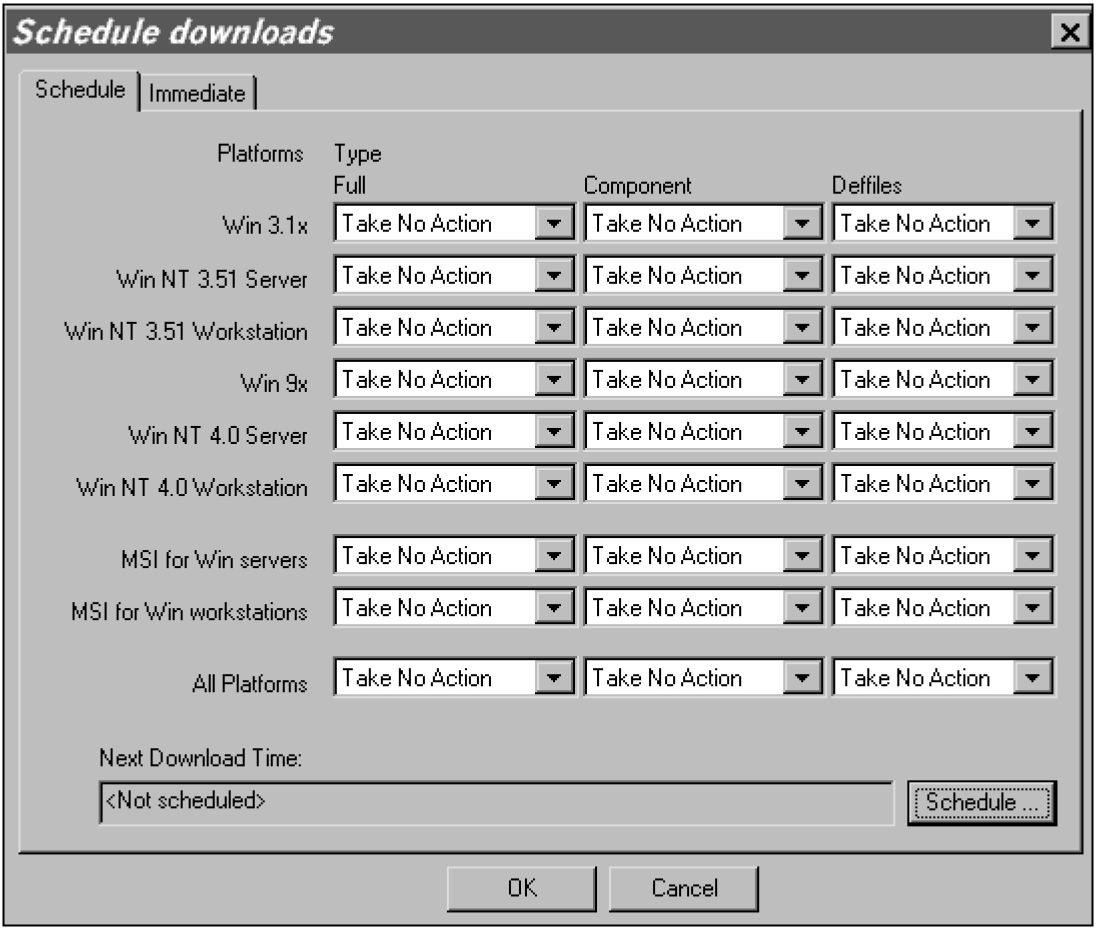
For Windows 95 and Windows NT 4.0, you must install Internet Explorer 4.0 or higher separately. If you did not install the Task Scheduler when you installed Internet Explorer 4.0, you can download a component update from the Microsoft site at:

http://www.microsoft.com/windows/ie/ie401/download/sp2/x86/en/download/setup.htm

NOTE: If you are setting up CSS Central for the first time or are changing any of the settings that you have previously selected, we recommend that you perform a manual (immediate) download of the Command AntiVirus files to test your settings. For more information, refer to **Performing a Manual Download**.

To set up scheduled downloads of the Command AntiVirus files into the CSS Central **staging directory** and then deploy them to the **automatic update directory**, follow these steps:

1. On the CSS Central menu bar, click **Automatic Update**. The system displays the drop-down menu.
2. Click **Schedule downloads**. The system displays the **Schedule downloads** dialog box:

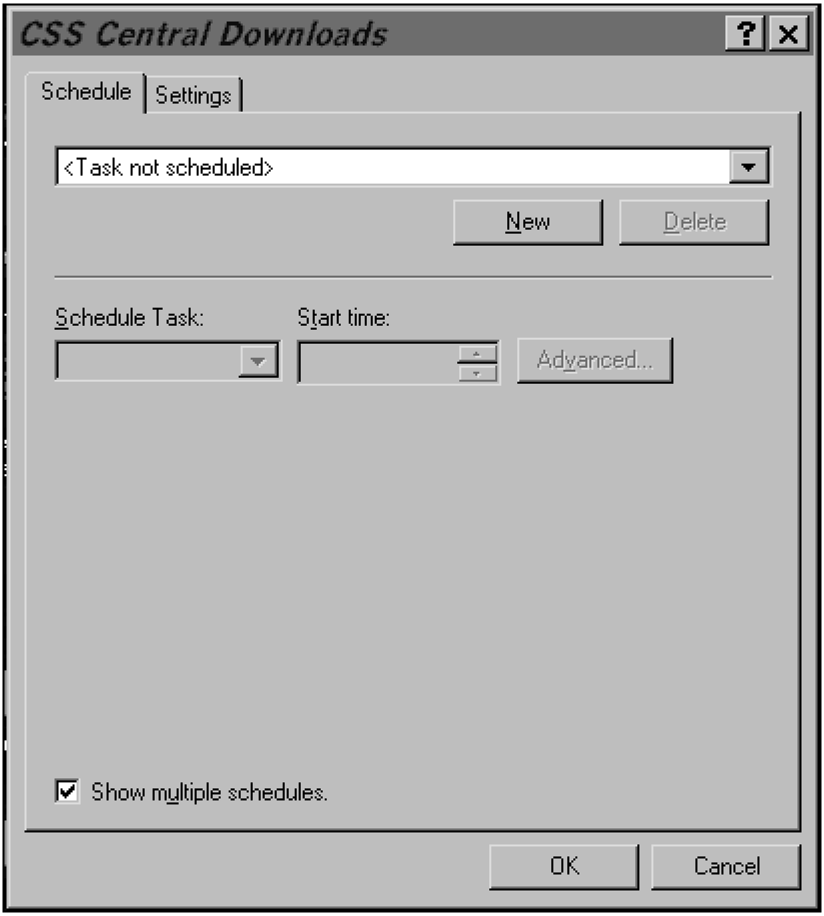


Platforms	Type		
	Full	Component	Deffiles
Win 3.1x	Take No Action	Take No Action	Take No Action
Win NT 3.51 Server	Take No Action	Take No Action	Take No Action
Win NT 3.51 Workstation	Take No Action	Take No Action	Take No Action
Win 9x	Take No Action	Take No Action	Take No Action
Win NT 4.0 Server	Take No Action	Take No Action	Take No Action
Win NT 4.0 Workstation	Take No Action	Take No Action	Take No Action
MSI for Win servers	Take No Action	Take No Action	Take No Action
MSI for Win workstations	Take No Action	Take No Action	Take No Action
All Platforms	Take No Action	Take No Action	Take No Action

Next Download Time: <Not scheduled>

Scheduled Downloads Dialog Box

3. In the **Schedule** dialog box under **Platforms Type**, locate the platform that you want to download.
4. In the **Full** list, click the drop-down arrow, and select **Download/Deploy**.
5. In the **Component** list, click the drop-down arrow, and select **Download/Deploy**.
6. In the **Deffiles** list, click the drop-down arrow, and select **Download/Deploy**.
7. To set the **Next Download Time**, click the **Schedule** button. The system displays the **CSS Central Downloads** dialog box:



<Task not scheduled>

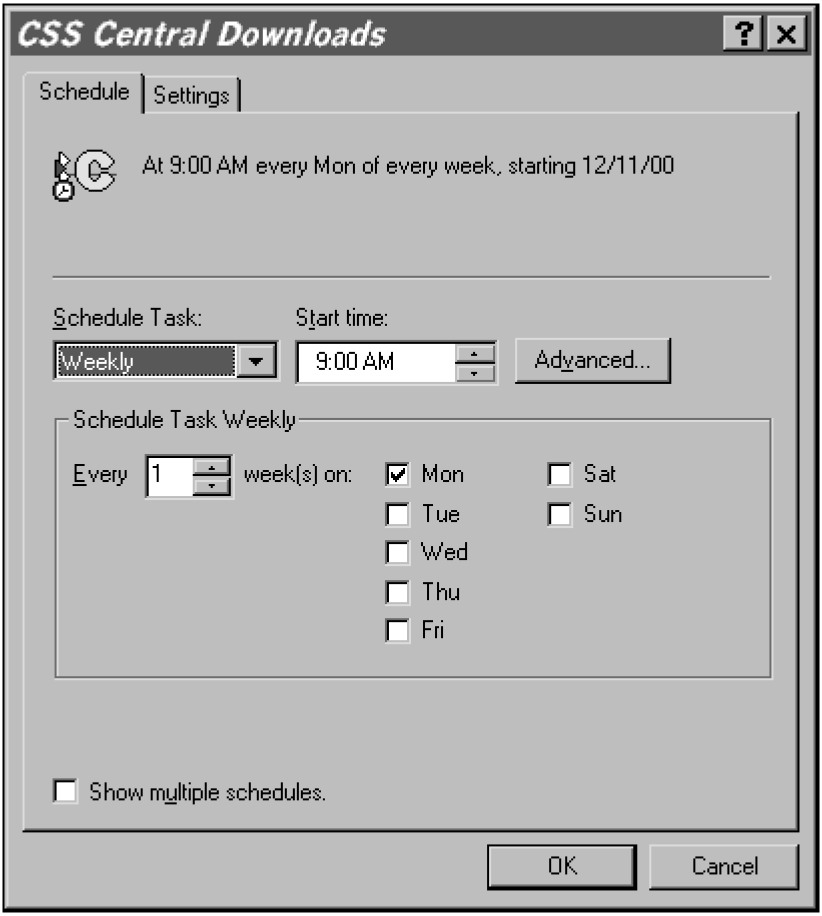
Schedule Task:

Start time:

☑ Show multiple schedules.

CSS Central Download Dialog Box

8. In the **CSS Central Downloads Schedule** dialog box, click **New**.
9. In the **Schedule Task** list, click the drop-down arrow and select how frequently you want the downloads to occur, for example, **Daily**, **Weekly**, **Monthly**, etc.



CSS Central Downloads

At 9:00 AM every Mon of every week, starting 12/11/00

Schedule Task: Weekly

Start time: 9:00 AM

Schedule Task Weekly

Every 1 week(s) on:

☑ Mon
□ Tue
□ Wed
□ Thu
□ Fri
□ Sat
□ Sun

□ Show multiple schedules.

CSS Central Downloads - Schedule Dialog Box

10. Depending on the selection that you made in **Step 9**, make the appropriate selections under **Schedule Task XXX**. For example, if you selected **Weekly**, under **Schedule Task Weekly**, select how often on a weekly basis and the day of the week that you want the downloads to occur.
11. In the **Start time** box, click the **up** or **down** arrows to select a time for the download to start.
12. Click **OK**. The system returns to the **Schedule downloads Schedule** dialog box. The scheduled time now appears in the **Next Download Time** text box.
13. If you setting up CSS Central for the first time, go to **Verifying the Deployment Status of Files** located later in this chapter.

Now, when an on-demand or scheduled update takes place, CSS Central does the following:

1. Downloads the update files from the download site to the **staging directory**.
2. Creates a CSAV product directory within the **automatic update directory**. The product directory is always a specific numeral. The following is an example of the product directory for CSAV for Windows 95/98/Me:

   ```
   \\SERVER\SHARE\UPDATE\0500
   ```

3. Creates separate subdirectories for the full-product updates, virus definition files, and the update component files. The definition files subdirectory ends in **.00**. The component files subdirectory ends in **.01**. The full-product subdirectory ends in **.02**. The file names are generated randomly by CSS Central. The following is an example of the path names to the **automatic update directory** and its subdirectories for CSAV for Windows 95/98/Me:

```
\\SERVER\SHARE\UPDATE\0500

\\SERVER\SHARE\UPDATE\0500\CSS43E.00

\\SERVER\SHARE\UPDATE\0500\CSS282.01

\\SERVER\SHARE\UPDATE\0500\CSS595.02
```

4. Decompresses the contents of the update file (full product, virus definitions, or component) into the appropriate directories in the **automatic update directory**.

NOTE: **<u>Every</u>** update creates a new subdirectory in the **automatic update directory**. Therefore, we recommend that you periodically delete old subdirectories.

5. Creates a file named CSSFILES.INI containing product-specific information. The following is an example of a CSSFILES.INI file for CSAV for Windows 95/98/Me:

```
[Win95-AntiVir]

BaseDir=\\SERVER\SHARE\UPDATE\0500

Fullprod=CSS595.02

Deffiles=CSS43e.00

Compont=CSS282.01
```

MANAGING DOWNLOADED AND DEPLOYED FILES

The options in the **Manage Downloaded/Deployed files** dialog box allow you to:

- Manually deploy the update files to the **automatic update directory**
- Review the update status log
- Delete update files from the **List of downloaded files**
- Deploy files that you did **<u>not</u>** download through CSS Central to the **automatic update directory**.
- Check the deployment status of files
- Edit the **SETUP.INI** file

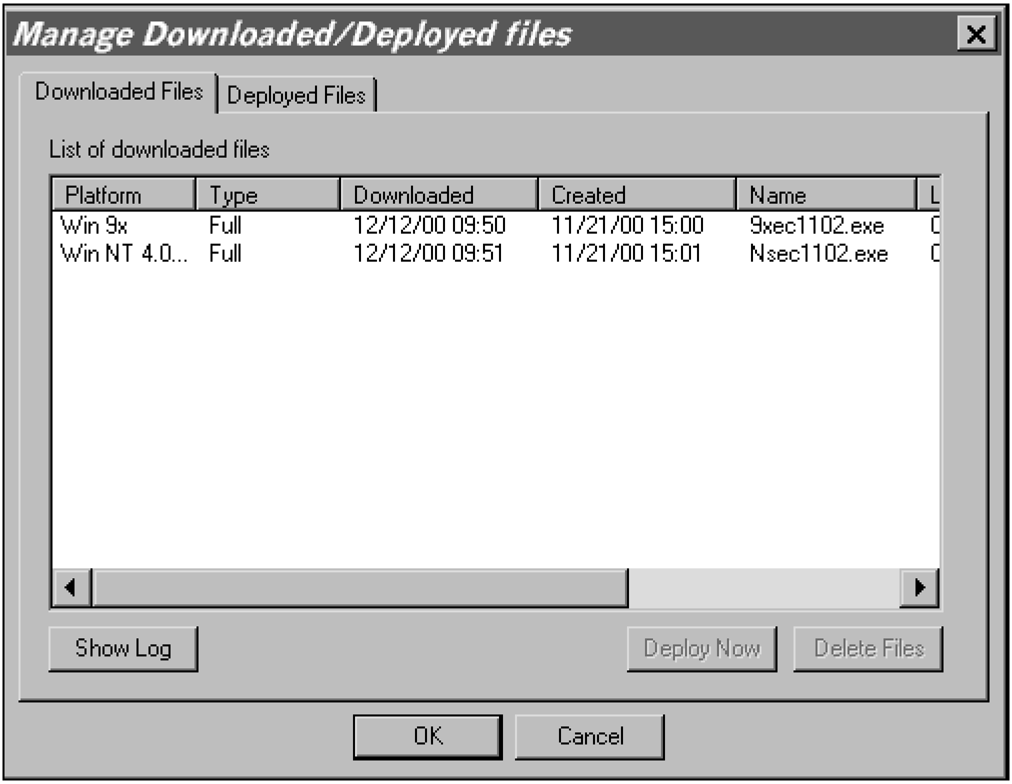
The **Manage Downloaded/Deployed files** dialog box contains two dialog boxes: **Downloaded Files** and **Deployed Files**. To access a specific dialog box, just click the appropriate tab.

Deploying the Downloaded Files to the Automatic Update Directory

If you did not previously select to automatically deploy the downloaded files to the **automatic update directory**, you can move the files manually through the **Manage Downloaded/Deployed files** dialog box.

To move the downloaded files to the **automatic update directory**, follow these steps:

1. On the CSS Central menu bar, click **Automatic Update**. The system displays the drop-down menu.
2. Click **Manage Downloaded/Deployed files**. The system displays the **Manage Downloaded/Deployed files** dialog box:



Platform	Type	Downloaded	Created	Name	L
Win 9x	Full	12/12/00 09:50	11/21/00 15:00	9xec1102.exe	C
Win NT 4.0...	Full	12/12/00 09:51	11/21/00 15:01	Nsec1102.exe	C

Manage Downloaded/Deployed Files – Downloaded Files Dialog Box

3. In the **Downloaded Files** dialog box locate the **Platform** and the **Type** of the download(s) that you want to deploy to the **automatic update directory**.

NOTE: To group the downloads by Platform or **Type**, click the appropriate column header.

4. Under **Platform**, click the platform name(s).
5. Click **Deploy Now**. The system displays a **Deployment Status** information box that confirms that the update file is being moved to the **automatic update directory**.

6. When the **Deployment Status** message box disappears, click **OK**.
7. Go to **Verifying the Deployment of Files**.

The **Downloaded Files** dialog box also allows you to:

- **Review the Status of the update log –** To review the status of the update log, click **Show Log**. This log documents the downloading of the update files to the **staging directory** and the deployment of these downloaded files to the **automatic update directory**.
- **Delete downloaded files** – To delete a set of downloaded files from the list, select the appropriate platform and type of files, and then click **Delete Files**.

Deploying Non-downloaded Files to the Automatic Update Directory

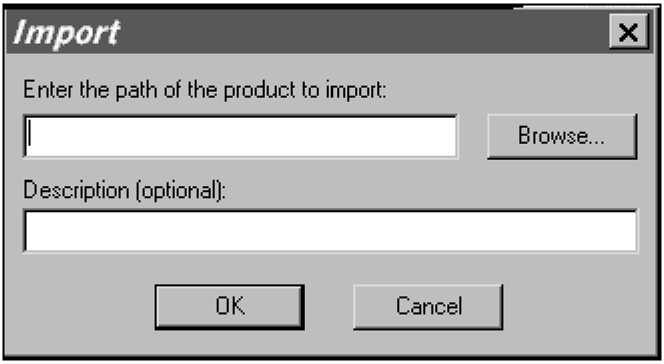
You may have a component update or a text file that you did not download through CSS Central but would like to distribute across the network.

The **Import** button allows you to associate the files to a particular platform and type in the **Platform** list. The files are copied to the **automatic update directory** and are ready to be rolled out over the network.

To move the non-downloaded files to the **automatic update directory**, follow these steps:

NOTE: If you have downloaded a ZIP or self-extracting file, you must first extract the files to a temporary directory.

1. On the CSS Central menu bar, click **Automatic Update**. The system displays the drop-down menu.
2. Click **Manage Downloaded/Deployed files**. The system displays the **Manage Downloaded/Deployed** dialog box.
3. Click the **Deployed Files** tab.
4. In the **Platform** list, click the drop-down arrow, and select a platform to which you would like to associate files.
5. Locate the appropriate text box, for example, **Full**, **Component**, or **Deffiles**, and click **Import**. The system displays the **Import** dialog box:



Import Dialog Box

6. In the **Enter the path of the product to import** text box, type the path to the file that you want to copy to the **automatic update directory.**

✓ **NOTE:** You can use the **Browse** button to search for the path. You can also type a description of the files that you are adding in the **Description** text box.

7. Click **OK**. The system returns to the **Deployed Files** dialog box.
8. Click **OK** to exit.
9. Go to **Verifying the Deployment Status of Files**.

Verifying the Deployment Status of Files

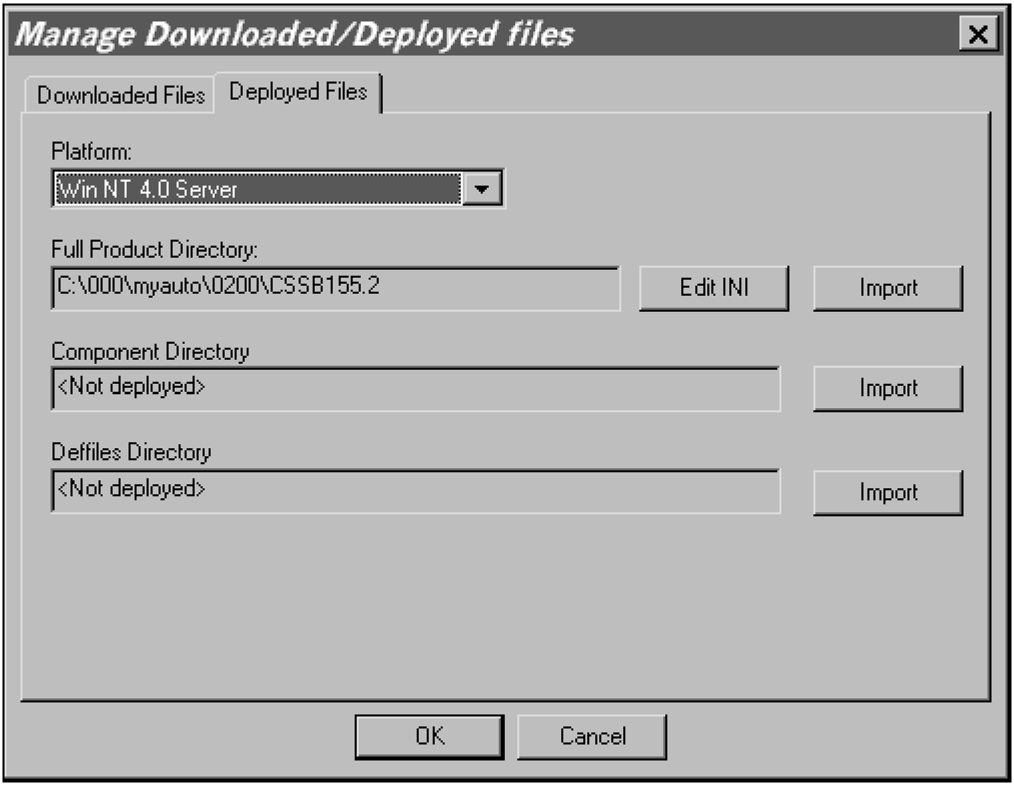
The **Deployed Files** dialog box allows you to verify the deployment status of files for each platform. You can also edit the **SETUP.INI** file and associate additional files to a particular platform.

To verify the deployment status of files, follow these steps:

1. On the CSS Central menu bar, click **Automatic Update**. The system displays the drop-down menu.

2. Click **Manage Downloaded/Deployed files**. The system displays the **Manage Downloaded/Deployed files** dialog box.

3. Click the **Deployed Files** tab. The system displays the **Deployed Files** dialog box:



Platform: Win NT 4.0 Server

Full Product Directory: C:\000\myauto\0200\CSSB155.2

Component Directory <Not deployed>

Deffiles Directory <Not deployed>

Manage Downloaded/Deployed Files – Deployed Files Dialog Box

4. In the **Platform** list, click the drop-down arrow, and select a platform for which you have just deployed update files to the **automatic update directory**. The status of update files for **full**, **component**, and **deffile** updates for this platform are displayed in the corresponding text boxes.

5. Verify that the appropriate update files are deployed to the **automatic update directory.**
6. If you are setting up CSS Central for the first time, go to **Editing the SETUP.INI File**.

Editing the SETUP.INI File

Before you can update your network computers, you **must** add the full UNC path to your **automatic update directory** to the **SETUP.INI** file. You may also want to make some additional configuration changes. Some of the common changes are outlined in **Step 8** of the following instructions.

If you are installing Command AntiVirus for NT/2000 or Command AntiVirus for Me, you must create an MST file to specify the path to your **automatic update directory** and to make any configuration changes. You can then add a reference to the MST file that you created in the **SETUP.INI** file.

NOTE: If you make any changes to the **SETUP.INI**, this **SETUP.INI** will be preserved when you update CSAV through CSS Central.

To make the changes, follow these steps:

1. On the CSS Central menu bar, click **Automatic Update**. The system displays the drop-down menu.
2. Click **Manage Downloaded/Deployed files**. The system displays the **Manage Downloaded/Deployed** dialog box.
3. Click the **Deployed Files** tab.
4. In the **Platform** list, click the drop-down arrow, and select a platform for which you have just deployed update files to the **automatic update directory**.
5. Click **Edit INI**. The system displays the **SETUP.INI** in a text editor.
6. If you are installing Command AntiVirus for NT/2000 or Command AntiVirus for Me, go to **Step 9**.

   If not, find: **AutoUpdateDir=**

7. After the equal sign (=), type in the full UNC path to your **automatic update directory**.

8. Make any additional configuration changes, and then go to **Step 10**. The following are some of the more common changes:

- Forces an installation without user intervention. The client gets the settings that you have provided.

  ```
  InstallSilent=YES
  ```

- Ensures an installation without user intervention. However, we recommend that the system administrator make at least one rescue disk.

  ```
  MakeRescueDisk=NO
  RunMakeRescueDisk=NO
  ```

- The “NET=FALSE” prevents your clients from repeatedly scanning network drives and slowing down the system.

  ```
  ;Setup options for the F-PROT32 program
  ;/DISINF=FALSE - Do not allow the user to disinfect
  ;/NET=FALSE - Do not allow the user to scan the
  network
  ;/DVP=FALSE - Do not allow the user to access active
  protection options
  Fpwcfg=/NET=FALSE
  ```

- Removes all macros if a variant is found. It will **not** remove all macros unless it finds a virus and cannot exactly identify it.

  ```
  ;Remove all macros when a virus is found.
  ;Note: Action on infection needs to be 3 for this
  option to work
  RemoveRemnants=YES
  ```

- This must be used with the “RemoveRemnants=YES” command above.

  ```
  ;0 is REPORT ONLY; 1 is DELETE; 2 is RENAME; 3 is
  DISINFECT
  ActionOnInfection=3
  ```

9. Add the following section to the SETUP.INI file:

```
[AUTOMATIC UPDATE]
COMMAND=
MST1=XXX1.MST
;MST2=XXX2.MST
```

NOTE: XXX1 and XXX2 represent the names of your MST file. If you are adding a second file, remove the semicolon (;) in front of MST2.

10. Save your changes and exit the file to return to the **Deployed Files** dialog box.
11. Click **OK** to exit.
12. **Go to Rolling Out CSAV Over the Network**.

ROLLING OUT CSAV OVER THE NETWORK

After the Command AntiVirus files are deployed to the **automatic update directory** either automatically or manually, you are ready to make the installation available to computers across your network. There are two ways to install Command AntiVirus to multiple computers. One uses your network's e-mail system. The other uses a network login script.

Through E-mail

To roll out CSAV using your mail system, follow these steps:

1. On the CSS Central menu bar, click **Remote Installation**. The system displays the drop-down menu.
2. Click **E-mail Installation** The system displays your e-mail address book.
3. From the recipient list, select the names or groups to whom you want the Command AntiVirus installation attachment sent, and add them to the **To** list.
4. Click **OK** or **Send** (depending on your mail client). The system displays the **Send Install To...** dialog box.
5. If necessary, modify the default text in the **Subject** and **Message** text boxes.

6. Click **OK** to send. The system returns to the **CSAV Neighborhood**.

✓ **NOTE:** To begin a standard CSAV installation to the local hard drive, mail recipients need only to double-click the **LOADER.EXE** attachment included with the e-mail message.

7. Go to **Creating a CSS Central Database**.

Through a NetWare Login Script

The following example of a NetWare login script provides code that you can modify and add to the end of your login script to roll out Command AntiVirus across your network.

The script looks for a specific file. If the file does **not** exist, the script terminates and runs the loader program from the CSS Central **automatic update directory.** This starts the installation of CSAV on the local computer. If the file exists, the installation is skipped and the login script continues processing.

For the script to run properly, you need to edit the [UserFiles] section in the SETUP.INI file for each CSAV platform being rolled out.

```
[UserFiles]

UserFile01=fp-###
```

The “#” represents the product version number. For example, “`fp-454`” stands for Command AntiVirus version 4.54.

When your customization is complete, go to **Creating a CSS Central Database**.

✓ **NOTE:** The bold-faced text in the following example must be modified to reflect conditions on your particular network. Comments are located after the semicolons.

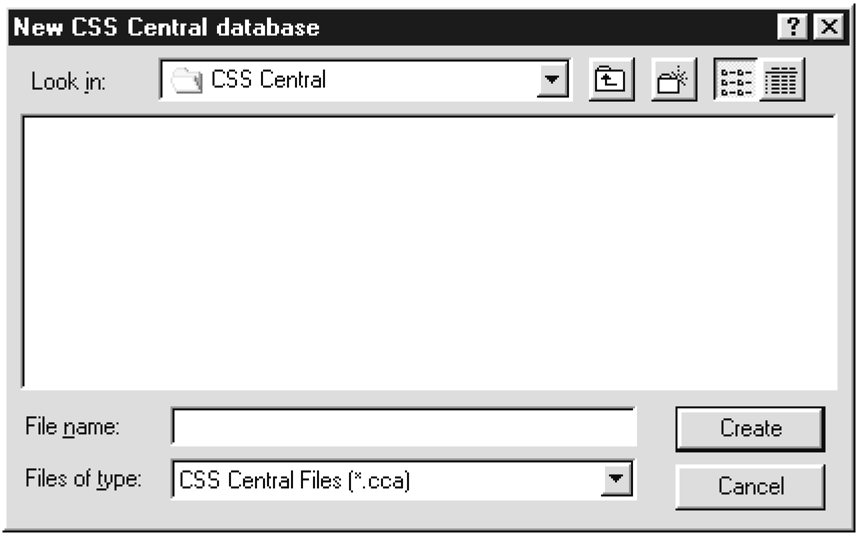
Example:

```
;------------------ START SCRIPT ------------------
;Start on the c: drive
Drive c:

;Try to display the version file
DISPLAY c:\progra~1\comman~1\f-prot95\fp-454
;If the version file does not exist, the error flag is
;set to non-zero
IF ERROR_LEVEL='0' THEN GOTO ENDSCRIPT

;Map a drive to the auto update directory (because exit
;only accepts 14 chars)
MAP ROOT f:=qa-312-nw\sys:crysorg\update

;Change drive and directory to the auto update directory
DRIVE F:

;Run the loader  (the file name must be 14 characters or
;less)
EXIT _loader.exe

ENDSCRIPT:

;---------------  END SCRIPT  ---------------
```

CREATING A CSS CENTRAL DATABASE

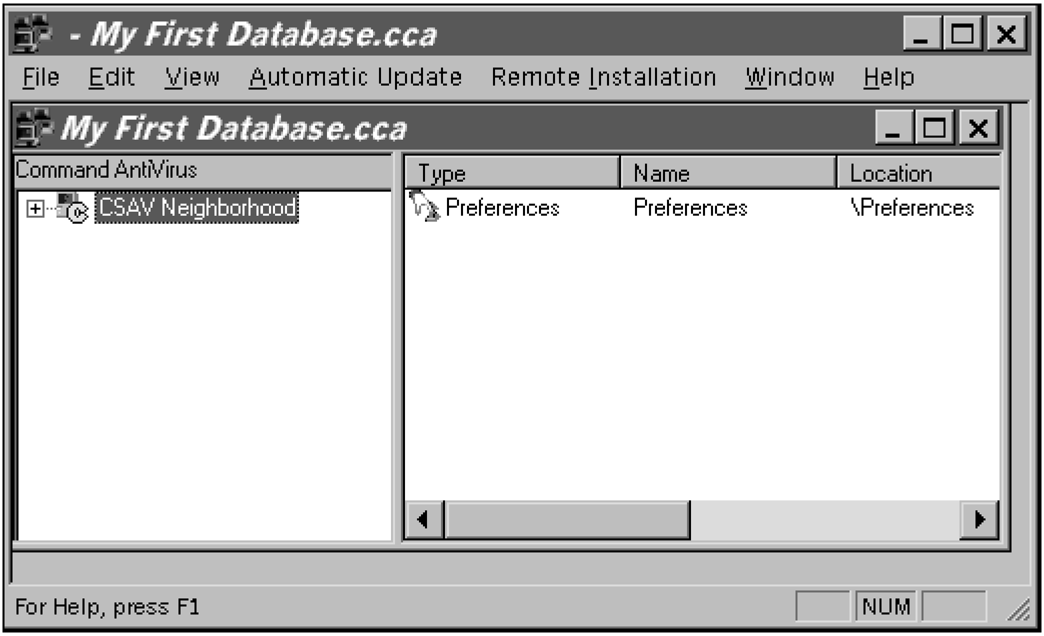
To administer Command AntiVirus on your network, you need to create a CSS Central database. This database allows you to maintain and change the Command AntiVirus settings for individual computers and computer groups. For more information, refer to **Administering CSAV on Your Network**.

1. Click the **Start** button.
2. Select **Programs**.
3. Select **Command Software**.
4. Click **CSS Central**.
5. On the CSS Central menu bar, click **File**. The system displays the drop-down menu.
6. Click **New**. The system displays the **New CSS Central database** dialog box:



New CSS Central Database Dialog Box

7. In the **File name** text box, type the name of the database that you want to create.
8. Click the **Create** button. The system displays the **CSAV Neighborhood** for your new database:



Type	Name	Location
Preferences	Preferences	\Preferences

CSAV Neighborhood

The name of the database appears in the title bar. All CSS Central databases have a .CCA extension.

The left pane contains CSAV Neighborhood with a plus sign (+) next to it. If you click the plus sign, the system displays **Preferences** below the neighborhood.

All computers and groups that are below **CSAV Neighborhood** inherit (take on) the existing preferences and tasks of **CSAV Neighborhood**. If you do **not** want the same tasks and preferences that the **parent** has, you can create new ones.

9. Go to **Administering CSAV on Your Network**.

ADMINISTERING CSAV ON YOUR NETWORK

Through CSS Central, you can maintain and change the Command AntiVirus settings for individual computers and computer groups. You can also create CSS Central databases for specific domains, locations and workgroups.

✓ **NOTE:** You can administer **only** computers that are running CSAV and that are turned on. If you try to administer a computer that is not running CSAV, you receive an error message.

ADDING COMPUTERS AND COMPUTER GROUPS TO YOUR CSS CENTRAL DATABASE

Before you can perform your administrative tasks, you must add the computers to be administered to the CSS Central database.

When adding computers and computer groups to your CSS Central database, you should add groups first and then individual computers. When you add a group, you can assign CSAV settings, also known as **preferences**, to the group. These **preferences** apply to all computers that are part of the group. Then, if necessary, you can change the CSAV settings for any individual computers in the group.

Creating CSAV Groups

CSS Central also allows you to put computers and/or groups of computers together in groups and subgroups called **CSAV groups**.

To create a **CSAV group** one level below **CSAV Neighborhood**, follow these steps:

1. In the left pane of the database window, select **CSAV Neighborhood**.
2. On the CSS Central menu bar, click **Edit**. The system displays the drop-down menu.
3. Click **New Group**. The system displays the **New Group** dialog box.

4. Type in the name of the new group that you want to create, for example, Accounting.
5. Click **OK**. The new group appears below **CSAV Neighborhood\Preferences**.

NOTE: To create a subgroup within Accounting, select **Accounting** and repeat **Steps 2** through **5**.

Adding Existing Computers and Domains

You can add an existing computer or domain to the **CSAV Neighborhood** or to a newly created **CSAV group** by **dragging and dropping** the selected item**.**

To add a computer or domain, follow these steps:

1. On the CSS Central menu bar, click **Edit**. The system displays the drop-down menu.
2. Click **Add Computer/Workgroup**. The system displays the **Add Computer or Workgroup** dialog box.
3. Click **Browse**. The system displays the Windows Explorer.
4. Resize Explorer and CSS Central so that both display on the desktop.
5. In Windows Explorer, select a computer or domain.
6. Press and hold down the left mouse button. Then, **drag** the selected item from Explorer and **drop** it onto **CSAV Neighborhood** or a **CSAV group**. Make sure that the target location is highlighted before you release the mouse button.

   The selected item appears with a platform-specific computer icon or a group icon below the target location.

Removing a Computer or CSAV Group from the Database

To remove a computer or CSAV group, follow these steps:

1. Select the item that you want to remove.
2. On the CSS Central menu bar, click **Edit**. The system displays the drop-down menu.
3. Click **Delete**. The system displays a dialog box asking you if you are sure you want to delete.
4. Click **Yes**. The selected item is removed.

MODIFYING THE CSAV PREFERENCES

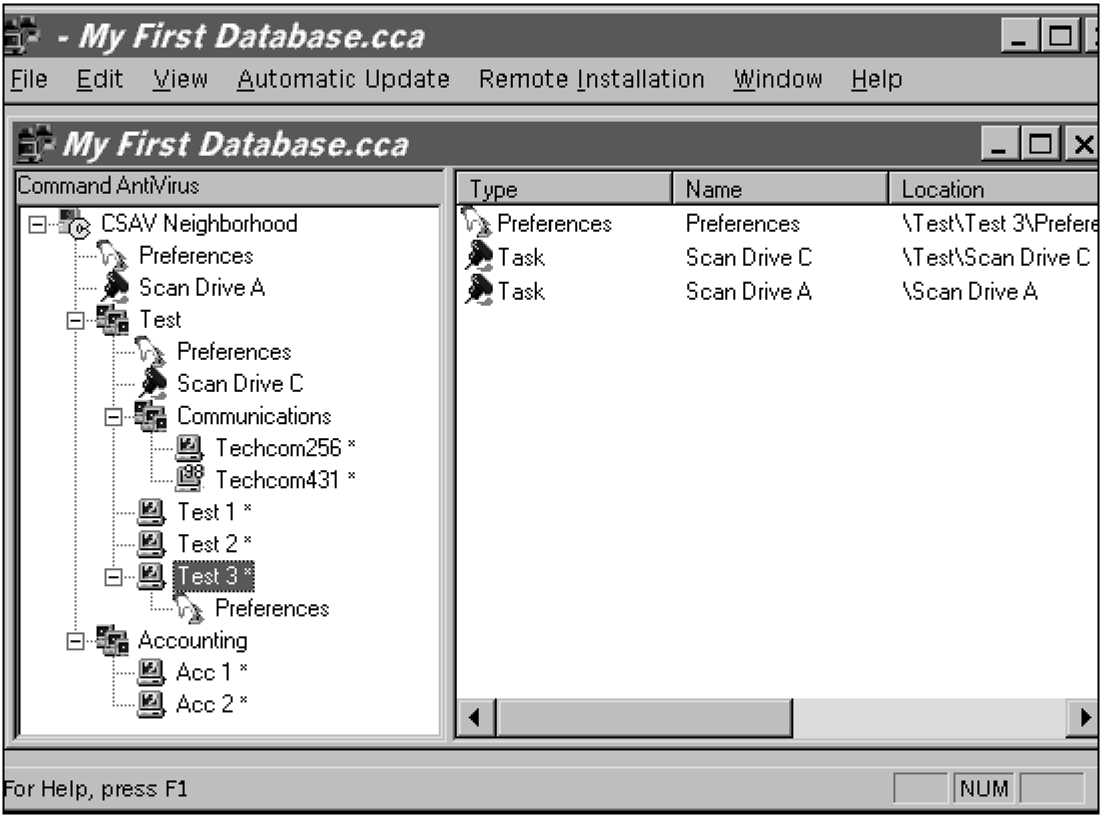
Each computer and CSAV group has a product configuration associated with it. This configuration is made up of CSAV settings and is called **Preferences**. There is only **one** set of **Preferences** for **each** computer or computer group.

The configuration for a particular computer or computer group is determined by its position in the tree view or by the presence of a **child** configuration item (task or preference) with its own settings.

All computers and groups that are below **CSAV Neighborhood** inherit (take on) the existing preferences and tasks of **CSAV Neighborhood**. If you do **not** want the same tasks and preferences that the **parent** has, you can create new ones.

Preferences for a computer or group replaces the **Preferences** of the **parent** groups.

For example, in the following **Database Window View**, the **Test 1**, **Test 2** and **Test 3** computers are part of the **Test** group. As the **Test** group has a particular set of preferences attached, the **Test** group’s **Preferences** replaces the default **Preferences** of **CSAV Neighborhood**. However, as the **Test 3** computer has a particular set of preferences attached, the **Test 3** computer’s **Preferences** replaces the **Test** group’s **Preferences** for only the **Test 3** computer.



Type	Name	Location
Preferences	Preferences	\Test\Test 3\Prefere
Task	Scan Drive C	\Test\Scan Drive C
Task	Scan Drive A	\Scan Drive A

For Help, press F1

Database Window View

If a computer icon is shown and there is not a particular set of preferences attached, the settings for that computer are the same as the **Preferences** of the group it is in.

For example, the **Test 1** and **Test 2** computers do not have any **Preferences** attached. Therefore, they take on the **Preferences** of the **Test** group.

If there is not a particular preference setting for the group, you can determine its settings by going up the tree until you reach a **parent** group that has **Preferences** attached.

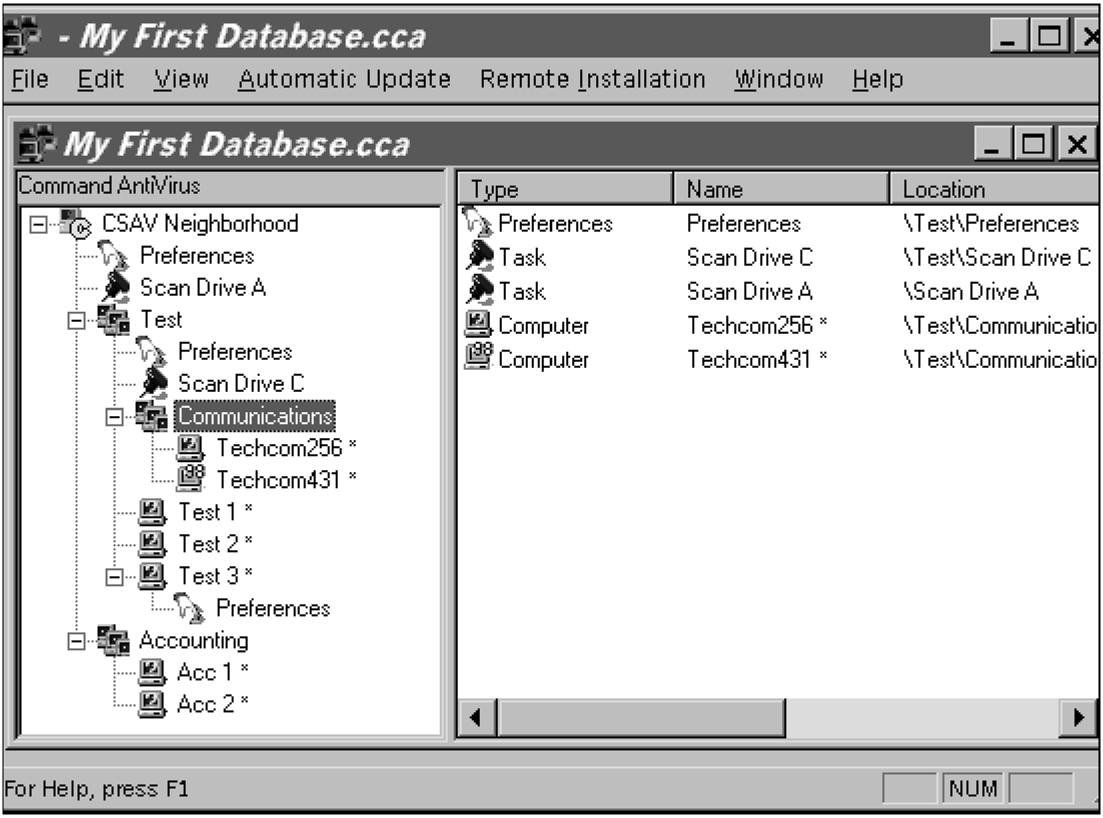
For example, the **Techcom256** and **Techcom431** computers are part of the **Communications** group. Neither the computers nor the group have a particular set of preferences attached. Therefore, the group and the computers take on the **Preferences** of the **Test** group.

If there is not a particular preference setting for a group or any of its **parent** groups or the group is not part of any other group, the default **Preferences** for the **CSAV Neighborhood** apply.

For example, the **ACC 1** and **ACC 2** computers are part of the **Accounting** group. Neither the computers nor the group have a particular set of preferences attached and they are not part of any other group. Therefore, the group and the computers take on the default **Preferences** of the **CSAV Neighborhood**.

Tasks for a computer or group include all tasks created for itself and for all of its **parent** groups.

For example, in the following **Database Window View**, the **CSAV Neighborhood** has a task to **Scan Drive A**, the **Test** group has a task to **Scan Drive C**, and the **Communications** group has no task assigned.



Type	Name	Location
Preferences	Preferences	\Test\Preferences
Task	Scan Drive C	\Test\Scan Drive C
Task	Scan Drive A	\Scan Drive A
Computer	Techcom256 *	\Test\Communicatio
Computer	Techcom431 *	\Test\Communicatio

Database Window View

As **Tasks** for a computer or group include all tasks created for itself and for all of its **parent** groups, the tasks for the **Test** and **Communications** groups and their computers include **Scan Drive A** and **Scan Drive C**.

NOTE: To display in the right pane the **Tasks** and the location of the **Preferences** for a particular computer or computer group, click the computer or group.

CSS Central allows you to remotely modify the CSAV **Preferences** of your network's computers. After changing the preferences in CSS Central, you can write those preferences to the computer groups that you select.

Remote control of CSAV preferences includes the following tasks. We recommend that you complete these tasks in the order that they are discussed.

- Viewing the current CSAV preferences
- Creating new preferences
- Modifying the preferences remotely
- Writing the new preferences to the remote system(s)

Viewing the Current CSAV Preferences

CSS Central allows you to view the current anti-virus preferences assigned to a computer or a computer group.

To view the currently assigned anti-virus preferences, follow these steps:

1. Click the plus sign (**+**) located to the left of the name.
2. Click the **Preferences** icon located just below the name. The system displays a list of preference settings for that computer or group.

NOTE: If there is no **Preferences** icon, click the computer or group to display in the right pane the location of the **Preferences** that apply. Double-click the **Preferences** icon in the right pane to display the list of preference settings.

Creating New CSAV Preferences

To create new **Preferences** for a computer or computer group, follow these steps:

1. Select the computer or computer group.
2. On the CSS Central menu bar, click **Edit**. The system displays the drop-down menu.
3. Click **New Preferences**. The system displays **Preferences** below the selected item. The settings are inherited from the preference group above.
4. To customize the settings, go to **Modifying CSAV Preferences Remotely**.

Modifying CSAV Preferences Remotely

To change the preferences for a computer or computer group, follow these steps:

1. Right-click the Preferences icon. The system displays a **Preferences Shortcut Menu**.
2. Click the **Preferences** option, for example, **Active Protection**, that you want to change. The system displays a dialog box for this setting.
3. Make the changes to the default settings.
4. Click **OK** to update the settings.
5. Repeat **Steps 2** through **4** for each option that you want to change.

NOTE: You can check the settings by clicking **Settings** on the **Preferences Shortcut Menu**.

Writing the New Preferences to the Remote System(s)

To write the new preferences for a computer or computer group to the remote system(s), follow these steps:

1. Select a computer or computer group.
2. On the CSS Central menu bar, click **File**. The system displays the drop-down menu.
3. To update **only** those computers marked with an asterisk (*) that are within the computers or groups that you selected, click **Write Remote Configurations Marked as Modified**. The system displays a caution dialog box asking you to confirm that you want to deploy the settings.
4. Click **Yes** to deploy the settings.

As the user on a remote computer running Windows 95/98/Me can always modify the system-wide settings from the **Preferences** menu, you may want to **lock** the remote computer.

To lock the preferences on a remote computer, follow these steps:

1. Select the computer.
2. On the CSS Central menu bar, click **Edit.** The system displays the drop-down menu.
3. Click **Lock/Unlock Computer**. The system displays a small padlock on the computer icon.
4. On the CSS Central menu bar, click **File**. The system displays the drop-down menu.
5. Click **Write Modified Remote Configuration**.
6. The system displays a caution dialog box asking you to confirm that you want to deploy the settings.
7. Click **Yes** to deploy the setting.

Copying Preferences

You can copy the preferences of one computer or computer group to another. To do this, follow these steps:

1. Select the **Preferences** icon that you want to copy.
2. Press and hold down the **CTRL** key. Then, use your mouse to **drag and drop** the selected icon on top of the target **Preferences** icon. The system displays a dialog box asking you to confirm that you want to copy the settings.
3. Click **Yes** to complete the copy.

INSTALLATION MAINTENANCE

After you have installed CSS Central, you can add or remove features, reinstall CSS Central, and remove CSS Central through the installation program's **Application Maintenance** dialog box.

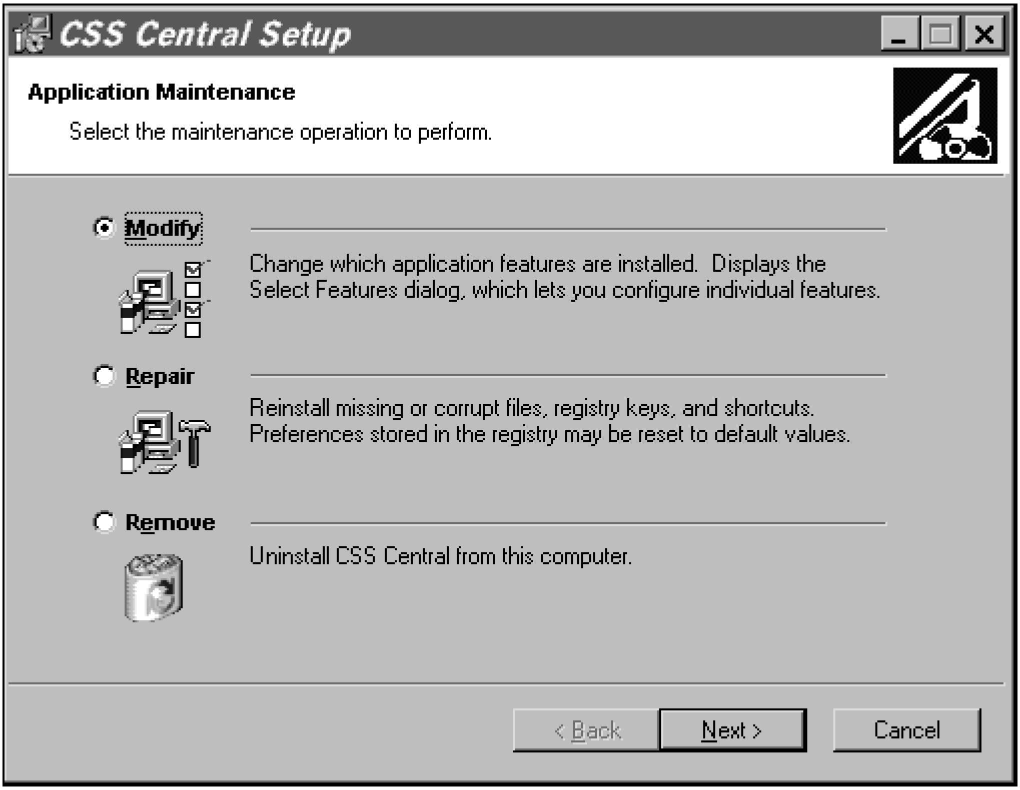
NOTE: In Windows 2000 and Windows Me, you can also remove CSS Central by clicking the **Remove** button in the Windows **Add/Remove Programs** dialog box.

To start the installation program, follow these steps:

1. Click the **Start** button on the Windows taskbar.
2. Select **Settings**.
3. Click **Control Panel**.
4. Double-click **Add/Remove Programs**. The system displays the **Add/Remove Programs** dialog box.
5. Select **CSS Central** from the list of currently installed programs.
6. In Windows 2000 and Windows Me, click the **Change** button.

   In Windows 9x and Windows NT, click the **Add/Remove** button.

   The system displays the CSS Central installation program's **Application Maintenance** dialog box:



CSS Central Setup

Application Maintenance

Select the maintenance operation to perform.

● **Modify**

Change which application features are installed. Displays the Select Features dialog, which lets you configure individual features.

○ **Repair**

Reinstall missing or corrupt files, registry keys, and shortcuts. Preferences stored in the registry may be reset to default values.

○ **Remove**

Uninstall CSS Central from this computer.

Application Maintenance Dialog Box

This dialog box contains the following operations:

- **Modify** – allows you to add or remove features or subfeatures.
- **Repair** – allows you to reinstall missing or corrupt files, registry keys, and shortcuts.

NOTE: Preferences stored in the registry may be reset to default values.

- **Remove** – allows you to remove CSS Central completely.

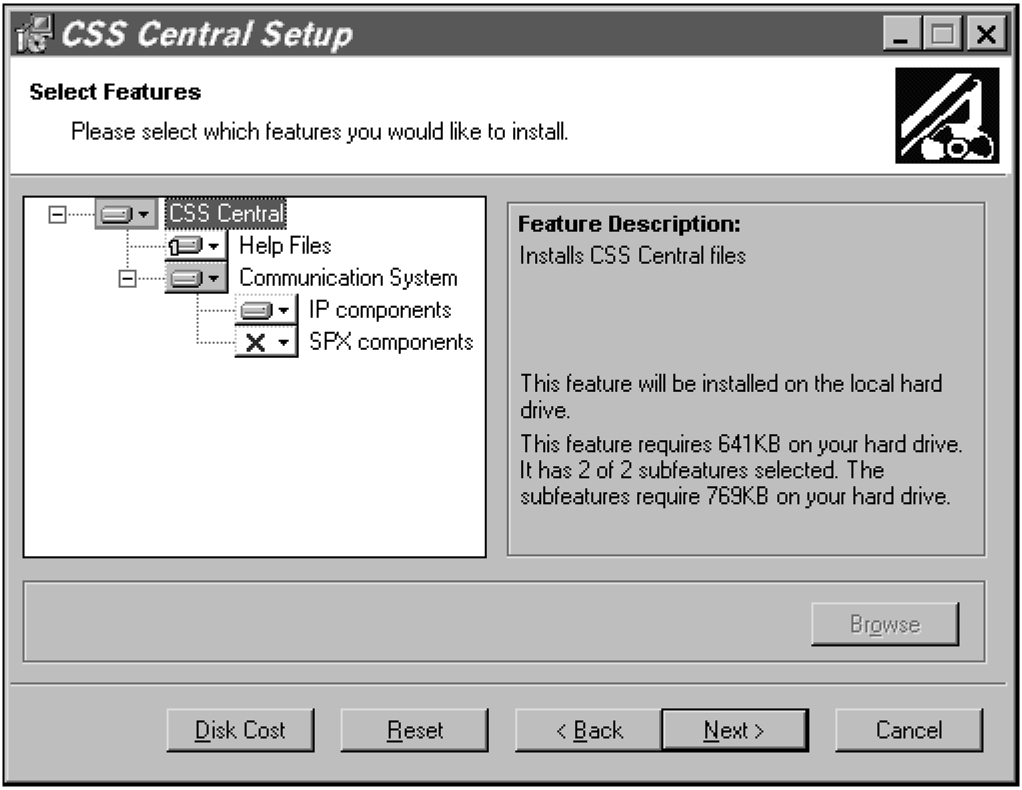
7. Go to the instructions for the operation that you want to perform, for example, **Adding or Removing Features**.

ADDING OR REMOVING FEATURES

After you have installed CSS Central, you can add or remove features through the installation program's **Application Maintenance** dialog box. Refer to **Steps 1** through **6** in the **Installation Maintenance** section located previously in this chapter.

To add or remove features, follow these steps:

1. In the CSS Central installation program's **Application Maintenance** dialog box, select **Modify** and click **Next**. The system displays the **Select Features** dialog box:



Feature Description:
Installs CSS Central files

This feature will be installed on the local hard drive.

This feature requires 641KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 769KB on your hard drive.

Select Features Dialog Box

2. Select or cancel the selection of the features or subfeatures that you want to add or remove. Click the plus signs (+) to display the subfeatures.

   To select a different installation state, click the down arrow to the right of the icon. For more information, refer to **Step 11** under **Installing** located previously in this chapter.

NOTE: To reset the features and subfeatures to the selections of the previous installation, click **Reset**. To view details of the amount of disk space that a feature or subfeature requires on the hard drive, click **Disk Cost**.

3. Click **Next** to begin.

NOTE: If you changed the Communication System subfeature that you want installed, the system displays the **Select Ports** dialog box. This dialog box allows you to change the default **IP Port** and **SPX Port** location numbers.

If you change the default port numbers in this dialog box, you should also change them when you install the same components in Command AntiVirus.

Type the new number in the appropriate text box and click **Next**.

NOTE: The installation program accepts only decimal values.

4. The system displays the **Updating System** dialog box. Please wait while the program copies the CSS Central files to your system.

NOTE: You can click **Cancel**, **Exit Setup** and then **OK** to cancel the installation and exit the setup program.

When the copying is complete, the system displays a dialog box informing you that CSS Central has been successfully installed.

5. Click **Finish** to exit.

REINSTALLING CSS CENTRAL

You can repair the CSS Central installation through the installation program's **Application Maintenance** dialog box. Refer to **Steps 1** through **6** in the **Installation Maintenance** section located previously in this chapter.

This option allows you to reinstall missing or corrupt files, registry keys, and shortcuts.

NOTE: Preferences stored in the registry may be reset to default values.

To reinstall CSS Central, follow these steps:

1. In the CSS Central installation program's **Application Maintenance** dialog box, select **Repair** and click **Next**. The system displays the **Ready to Repair the Application** dialog box.

NOTE: You can click **Back** to make a new selection, or you can click **Cancel**, **Exit Setup** and then **OK** to cancel the reinstallation and exit the setup program.

2. Click **Next** to begin the installation. The system displays the **Updating System** dialog box. Please wait while the program copies the CSS Central files to your system.

NOTE: You can click **Cancel**, **Exit Setup** and then **OK** to cancel the reinstallation and exit the setup program.

3. When the copying is complete, the system displays a dialog box informing you that CSS Central has been successfully installed. Click **Finish** to exit.

REMOVING CSS CENTRAL

You can completely remove an installed version of CSS Central through the installation program's **Application Maintenance** dialog box. Refer to **Steps 1** through **6** in the **Installation Maintenance** section located previously in this chapter.

To remove CSS Central completely, follow these steps:

1. In the CSS Central installation program's **Application Maintenance** dialog box, select **Remove** and click **Next**. The system displays the **Uninstall** dialog box.
2. Click **Next** to remove CSS Central. The system displays the **Updating System** dialog box. Please wait while the program removes the CSS Central files from your system.

NOTE: You can click **Cancel**, **Exit Setup** and then **OK** to cancel the uninstall and exit the setup program.

3. When the removal is complete, the system displays a dialog box informing you that CSS Central has been successfully uninstalled. Click **Finish** to exit.

GLOSSARY

BOOT SECTOR

Stores critical drive information. Floppy disks and local hard disks have boot sectors.

BOOT SECTOR VIRUS

A virus that infects the boot sector of a hard disk or a floppy disk. Note that any formatted disk (even one that is blank or contains only text data) can contain a boot sector virus. Booting with an infected disk activates this type of virus.

CIRCULAR INFECTION

A type of infection that occurs when two viruses infect the boot sector of a disk, rendering the disk unbootable. Removing one virus usually causes a re-infection with the other virus.

CMOS

Complimentary Metal Oxide Semi-Conductor. CMOS stores critical configuration information. Some viruses try to alter this data.

COMPANION VIRUS

A virus that infects executable files by creating a companion file with the same name but with a .COM extension. As DOS executes .COM files before .EXE files and .BAT files, the virus loads before the executable file.

CROSS-LINKED FILES

Cross-linking, a common situation rarely associated with viruses, occurs when two files seem to share the same clusters on the disk.

DROPPER

A program compressed with PKLite, Diet, LZExe, etc... that contains a virus. Microsoft Word documents can also function as droppers. A dropper deposits the virus onto a hard disk, a floppy disk, a file or into memory. The children of this process are not droppers.

EICAR TEST FILE

EICAR (European Institute for Antivirus Research) test file provides an industry standard solution to test anti-virus products. The EICAR test file is the result of a cooperative effort between various anti-virus researchers. You can use this file in a variety of ways. For example, you can safely verify that real-time protection is active and demonstrate what happens when it finds a virus.

ENCRYPTION

A process of making data unreadable. Some viruses use encryption techniques in order to hide their presence from anti-virus scanners.

EXECUTABLE CODE

Instructions that a computer uses to accomplish various tasks. This includes COM, EXE, DLL and similar files. In a broader sense, executable code includes the code found in disk boot sectors, batch files and even macros used by some applications.

FALSE POSITIVE

A false positive occurs when a scanner identifies a file as infected when, in fact, the file is virus-free.

FILE STEALTH

A virus characteristic that hides the increase in length of infected files. For example, if the original size of a file is 240 KB, the file would appear to remain the same size although the file now contains a virus.

FULL STEALTH

A virus that tries to hide its presence on an infected system. When operational, a full stealth virus can evade attempts to search for it in files or memory.

HEURISTICS

A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures.

The advantage of the heuristics scan is that new variants of existing viruses cannot fool it. However, heuristics scans occasionally report suspicious code in normal programs. For example, the scanning of a program may generate the following message:

```
C:\DOS\MSHERC.COM has been modified by adding some code
at the end. This does not appear to be a virus, but
might be a self-checking routine or some "wrapper"
program.
```

Command AntiVirus issues a stronger warning based on the likelihood of a program actually containing a virus.

INTEGRITY CHECKER

A program that checks for changes to files. Integrity checkers, when used correctly, can provide an excellent second line of defense against new viruses or variants.

JOKE PROGRAMS

A program that makes the computer behave oddly. Command AntiVirus detects the presence of several well-known joke programs. While joke programs are generally harmless, their side effects are often mistaken for those of a virus.

LOGIC BOMB

A program that runs a pre-programmed routine (frequently destructive) when a designated condition is met. Logic bombs do not make copies of themselves.

MALWARE

A generic name for software that intentionally performs actions that can damage data or disrupt systems.

MACRO VIRUS

A virus written in one of the many macro languages. The macro viruses spread via infected files such as documents, spreadsheets, databases, or any computer program that uses a macro languages.

MASTER BOOT RECORD (MBR)

The first physical sector on all PC hard disks reserved for a short bootstrap program. The MBR also contains the partition table.

MEMORY-RESIDENT

Residing in computer memory as opposed to on the disk.

MULTIPARTITE

A virus that is able to infect both files and boot sectors. Such viruses are highly infectious.

ON-ACCESS SCAN

A virus scan that starts when the operating system performs an action on a file. For instance, when a file is created on the hard disk, Command AntiVirus' on-access protection scans it immediately. If a virus is detected, CSAV performs the action you specified in the on-access scan task settings.

ON-DEMAND SCAN

A virus scan that is started manually. In Command AntiVirus, on-demand scans can also be configured to scan automatically at a specified time (see the glossary entry for **Scheduled Scan**).

PARTITION TABLE

A place on a hard disk containing information required to access the partitions (logical blocks) of a PC disk. The partition table also contains a flag indicating which partition should be used to boot the system (the active partition). The partition table is stored in the master boot record (MBR).

POLYMORPHISM

A virus in which the code appears to be different every time the virus reproduces (though generally each reproduction of the virus is functionally identical). This process is usually achieved by encrypting the body of the virus and adding a decryption routine that is different for each reproduction.

SCHEDULED SCAN

An on-demand scan that is configured to run automatically each day, once a day on specified days of the week, or once a month on a given date.

STEALTH VIRUS

A virus that tries to hide itself. Changes made by this virus are not easily detected. For example, if the original size of a file is 240K, the infected file would appear to remain the same size. A stealth virus can operate only when it is resident in memory.

TROJAN (OR TROJAN HORSE)

A program that carries out an unauthorized function while hidden inside an authorized program. This program is designed to do something other than what it claims to and frequently is destructive in its actions.

GLOSSARY

TUNNELING

A characteristic of some viruses that try to access the operating system directly, bypassing any TSRs (including anti-virus software) that have been loaded.

VIRUS

An independent program that reproduces itself. A virus may attach to other programs; it must create copies of itself (see the glossary entry for **Companion Viruses***).* It may attach itself to any executable code, including but not limited to boot sectors and/or partition sectors of hard and/or floppy disks. It may damage, corrupt or destroy data, or degrade system performance.

VIRUS SIMULATOR

A program that creates files that “look like” viruses. Such files are useless for testing purposes because they are not really infected. Command AntiVirus is smart enough not to be fooled by a simulator.

VIRUS VARIANT

A modification of a previously known virus, a variation.

WORM

A program that reproduces by copying itself over and over, system to system. Worms are self-contained and generally use networks to spread.

APPENDIX

The following section contains a list of messages that might appear in the Windows Event Viewer.

EVENT ID DESCRIPTIONS

In the Windows Event Viewer, CSS AV Scheduler (CSS-AVS.EXE) logs event messages to the Application Log and CSS DVP (CSS-DVP.SYS) logs events to the System Log. The list below contains the Event ID code numbers and their corresponding message descriptions. The event messages that are logged in Event Viewer can refer to (1) actions taken when a virus is found, (2) system-related problems or (3) routine system functions. Event Viewer messages can be viewed by double-clicking your cursor on a message line in either of the above-mentioned log files. You will then be presented with an Event Details information box that contains the Event ID’s full message.

If, for some reason, the service file (CSS-AVS.EXE) gets deleted or becomes corrupted, the Event Details information box will contain the Event ID code number, but not a description of the message for that code number.

Event ID=210

Message: AV Scheduler Service Install Failed.

Cause: The most likely cause of this message is that the service is already installed.

Effect: If this message appears because of a prior installation of the service, then there will be no effect.

Solution: None required.

Event ID=211

Message: AV Scheduler Service Installation Completed.

Cause: This is an informational message notifying the user that the service has successfully been installed on the system

Effect: None.

Solution: None required.

Event ID=212

Message: AV Scheduler Service Started.

Cause: This is an informational message notifying the user that the service has successfully been started on the system.

Effect: None.

Solution: None required.

Event ID=213

Message: AV Scheduler Service Stopped.

Cause: This is an informational message notifying the user that the service has stopped. The service, in most instances, would have been terminated manually by the user.

Effect: None.

Solution: None required.

Event ID=214

Message: Archive file is corrupted or cannot be accessed. [Filename.zip]

Cause: The ZIP file may have been corrupted during a file copy or during the compression process. It may also have been saved to a physically bad section of the disk. Another possible cause is that the zipped file may be password protected.

Effect: The file cannot be successfully unzipped. As such, it cannot be scanned for viruses.

Solution: Use PKZipFix to repair the damaged file. The file in question is shown at the end of the message. If the file cannot be repaired, replace the damaged copy of the file with an uncorrupted copy of the file if possible. If the zipped file was password protected, then use the password to unzip the file and then perform a manual scan of the file.

Event ID=215

Message: AV Scheduler Service cannot communicate with Kernel Mode Driver.

Cause: The DVP Kernel Mode Driver has either been removed or it was not successfully installed. Another reason for the message can be that the kernel mode driver has been intentionally disabled by a user.

Effect: Dynamic Virus Protection will not function and scheduled scans will not take place.

Solution: Check the folder that should contain the kernel mode driver. If the driver is missing, either reinstall Command AntiVirus or manually copy the driver to the proper folder.

If the kernel mode driver was found in the proper folder, using ScanDisk or a similar utility, check Command AntiVirus installation diskettes for physical defects. If a defect is found, discard the defective diskette and create a replacement for it. Once a replacement has been made, reinstall Command AntiVirus.

Finally, if it appears that the driver has been intentionally disabled, be sure to enable it once again.

Event ID=216

Message: AV Scheduler Service cannot start -- Registration failed.

Cause: A problem occurred during installation. The NT registry could be corrupted or another internal NT process failed during the Command AntiVirus installation process. Another possible reason for the message is that the service is already installed and running.

Effect: The service cannot start as it could not be registered in the NT Control Panel “Services” applet.

Solution: Boot from an emergency disk and instruct it to repair the registry.

Event ID=217

Message: AV Scheduler Service cannot report to Service Control Manager.

Cause: The Service-related entries in the registry may not be correct. Also, the Service’s executable may be corrupted. Further, the Service Control Manager (SCM) may have been too busy dealing with another service for a successful report to take place. Another possible cause would be that the SCM component in Windows has failed.

Effect: The user will not be able to start, stop, pause or continue AV Scheduler as necessary.

Solution: Check the registry to make sure that AV Scheduler’s settings are correct. Also, make sure that the executable, CSS-AVS.EXE, is not corrupt. If those two areas reveal no problems, then reboot the system and see if that reboot solves the AV Scheduler-related problem. If you still encounter problems after the reboot, the SCM component may be damaged. If this appears to be the case, contact the Microsoft Corporation for assistance.

Event ID=218

Message: AV Scheduler Service has been terminated normally.

Cause: This is an informational message informing the user that the service has been successfully shut down.

Effect: None.

Solution: None required.

Event ID=219

Message: AV Scheduler Service cannot find Application Location path in registry, “TaskLocation” key Missing.

Cause: The Application Location path in the Windows registry is either corrupted or it has been removed. The problem could have been caused either by a problem that was encountered during Command AntiVirus’ installation or by a later corruption of the registry.

Effect: The scheduler service will not run.

Solution: Restore the missing path in the Windows registry. To restore the path, in the registry follow “HKEY_Local_Machine\Software\Command Software\F-PROT32”. Then for the “Location” value, enter the proper value. In this case, the value will simply be the folder into which the program was installed.

Event ID=220

Message: AV Scheduler Service cannot find any task to schedule.

Cause: The service does not have read/write access to profiles or tasks that should be available to it. Two possible causes include (1) all the FPT files were deleted or (2) the profiles or tasks could not be read, perhaps due to a security program or some other such application or utility.

Effect: The service will run. However, although it is running, no tasks will be executed.

Solution: Change the access attributes to the profiles and/or tasks in question so that the service can read and write to them. If the FPT files were deleted, then they will need to be recreated. If another program is denying read/write access to the profiles or tasks, then that program will need to be modified so that such access is possible.

Event ID=221

Message: AV Scheduler Service is Out of Memory.

Cause: There are several reasons why this message can occur. For instance, too many programs may be open at once. Second, the machine may not have enough RAM. Also, some programs that have been closed may, nonetheless, still be occupying some RAM (this is known as RAM “leakage”).

Effect: The effected program will not run.

Solution: To start, free up some memory by shutting down the most nonessential programs. If any unnecessary programs or utilities are being loaded in the StartUp folder, consider removing them. Also, be certain that the system has sufficient RAM to run all necessary programs.

Event ID=222

Message: AV Scheduler Service has failed running a scan task because of low resources.

Cause: The causes for this message are very similar to those for the “Out of Memory” message. Too many programs may be open at once. That is, the system may not have enough RAM to run more than a certain number of programs. Another possible cause could be that some programs, despite their having been closed, may still be occupying some parts of memory, thus reducing the amount of available system resources.

Effect: The effected program will not run.

Solution: Terminate the most non-essential programs to free up some memory. If any unnecessary programs or utilities are being loaded in the StartUp folder, consider removing them. Also, be certain that the system has sufficient RAM to run all necessary programs.

Event ID=223

Message: AV Scheduler Service has been Suspended.

Cause: This is an informational message indicating that the service has been successfully paused.

Effect: None.

Solution: None required.

Event ID=224

Message: AV Scheduler Service has been resumed and is running.

Cause: This is an informational message indicating that the service has been successfully resumed after a pause or other interruption.

Effect: None.

Solution: None required.

Event ID=225

Message: AV Scheduler Service has failed to get a scan thread from kernel mode driver.

Cause: Too many applications are trying to communicate with the kernel-mode driver at the same time.

Effect: The service cannot ask the kernel-mode driver to perform a scan or other tasks.

Solution: Retry the operation at a later time.

Event ID=226

Message: The AV Scheduler Service has been Stopped while Running a Task.

Cause: This is an informational message informing the user that the scheduler has stopped during the execution of a task. The task itself will be terminated as well.

Effect: None.

Solution: None required.

Event ID=227

Message: Error Terminating Thread.

Cause: This is an informational message informing the user that the scan thread could not be terminated manually. The thread will continue to task until it terminates automatically.

Effect: None.

Solution: None required.

Event ID=228

Message: Error Communicating with Service Control Manager.

Cause: The SCM may have trapped or abended. Alternatively, the SCM may have been too busy to respond to messages.

Effect: The SCM information panel information would not be updated with the current status of the service.

Solution: Shutdown the scheduling service (CSS-AVS.EXE) and then restart it. Another solution would be to reboot the system.

Event ID=229

Message: AV Scheduler Service Uninstall Failed.

Cause: The Service Control Manager would not allow the service to be uninstalled. This could be caused by some problem in the registry. Another possible cause could be a previously failed uninstall that left remnants of the service on the system. Also, this message can appear if the service has already been uninstalled. In other words, if the service is already uninstalled and you mistakenly try to uninstall the service, this message could appear.

Effect: The scheduling service will not execute as desired.

Solution: As the service can still be partially installed, a manual uninstall is required. If you reinstall the service after having manually uninstalled it, be sure to reboot the system so that all necessary files will be properly updated.

Event ID=230

Message: Unable to get status of AV Service.

Cause: This is an informational message informing the user that the main process thread of the service was unable to get information regarding the status of a subprocess, if any.

Effect: None.

Solution: None required.

Event ID=231

Message: An error occurred while stopping the AV service.

Cause: A process interfered with the proper termination of the service. This error message can also appear if the service was not running when the user attempted to “stop” the service.

Effect: The service will continue to run. However, it is unlikely that scheduled scans will continue.

Solution: The Service Control Manager (SCM) will contain information regarding the cause of the error. Use the information from the SCM to locate and troubleshoot the cause of the problem. In the short-term, simply restarting the system will often correct the problem.

Event ID=232

Message: AV Scheduler Service has been removed.

Cause: This is an informational message informing the user that the service has been successfully removed from the system.

Effect: None.

Solution: None required.

Event ID=233

Message: While scanning a File, AV Driver reports: [Item Scanned] Action=[Action Taken on the Item Scanned], Result=[Optional Information on the Action Taken].

Cause: This is an informational message informing the user that, when a particular file was scanned, an action was performed on the file. Optional information regarding the action that was taken is also reported.

Effect: None.

Solution: None required.

Event ID=234

Message: While scanning the MBR, AV Driver reports: [Item Scanned] Action=[Action Taken on the Item Scanned], Result=[Optional Information on the Action Taken].

Cause: This is an informational message informing the user that, when the Master Boot Record (MBR) was scanned, an action was performed on the MBR. Optional information regarding the action that was taken is also reported.

Effect: None.

Solution: None required.

Event ID=235

Message: While scanning Memory AV Driver reports: [Item Scanned] Action=[Action Taken on the Item Scanned], Result=[Optional Information on the Action Taken].

Cause: This is an informational message informing the user that, when memory was scanned, an action was performed upon it. Optional information regarding the action that was taken is also reported.

Effect: None.

Solution: None required.

Event ID=236

Message: AV Scheduler Service cannot find Additional tasks path in registry, “Additional Tasks” Key Missing.

Cause: This is an informational message informing the user that the “Additional Tasks” key has been removed from the registry.

Effect: None.

Solution: None required. F-Agent will recreate this missing key automatically when the next inactivity scan takes place. However, if this message appears persistently in the Windows Event Viewer, call Command Software Systems Technical Support for assistance.

Event ID=237

Message: AV Scheduler Service cannot find User Profiles path in registry. 'ProfilePath' Key Missing.

Cause: The “ProfilePath” key has been removed from the registry or its entry in the registry has been corrupted. This may have been caused by either an improper disk write or by a faulty installation.

Effect: The user’s scheduled tasks cannot run.

Solution: Restore the “ProfilePath” key in the registry by adding the following key to the NT registry:

HKEY_LOCAL_MACHINE/SOFTWARE/Command Software/F-PROT32

Then, for the “Profile Path” item, enter the value of:

C:\WINNT40\Profiles\%s\Command Software\F-PROTNT\Tasks

Event ID=238

Message: Scheduled Scan of [Task Name] Started.

Cause: This is an informational message informing the user that a particular scheduled scanning task has started.

Effect: None.

Solution: None required.

Event ID=239

Message: Schedule Scan of [Task Name] Completed.

Cause: This is an informational message informing the user that a particular scanning task has been completed.

Effect: None.

Solution: None required.

Event ID=240

Message: Scheduled Scan Task Information has been reloaded.

Cause: This is an information message informing the user that task information regarding a scanning task has been successfully reloaded.

Effect: None.

Solution: None required.

Event ID=241

Message: Scheduled Scan Task Information has been updated by Command AntiVirus.

Cause: This is an informational message informing the user that the Scheduled Scan Task information was revised by Command AntiVirus.

Effect: None.

Solution: None required.

Event ID=242

Message: F-Agent has requested an Inactivity Task Scan.

Cause: This is an informational message informing the user that Command AntiVirus requested a scan after “x” number of minutes of keyboard or mouse inactivity.

Effect: None.

Solution: None required.

Event ID=243

Message: AV Scheduler Service Received a Device IOCTL Error while scanning the MBR.

Cause: The CSS-DVP.SYS and CSS-AVS.EXE files may be from two different releases. If this is the case, then service probably sent bad parameters to the kernel-mode driver.

Effect: The parameters passed to the kernel-mode driver will not take effect.

Solution: Make sure that CSS-DVP.SYS and CSS-AVS.EXE are from the same release.

Event ID=244

Message: AV Scheduler Service Received a Device IOCTL Error while scanning Memory.

Cause: As with Event ID 243, the CSS-DVP.SYS and CSS-AVS.EXE files may be from two different releases. If this is the case, then service probably sent bad parameters to the kernel-mode driver.

Effect: The parameters passed to the kernel-mode driver will not take effect.

Solution: Make sure that CSS-DVP.SYS and CSS-AVS.EXE are from the same release.

Event ID=245

Message: AV Scheduler Service Received a Device IOCTL Error while scanning a File.

Cause: There was an error communicating with the dynamic virus protection driver (DVP). The CSS-DVP.SYS and CSS-AVS.EXE files may be from two different releases. If this is the case, then service probably sent bad parameters to the kernel-mode driver. Another possible cause could be that the driver, CSS-DVP, could be either stopped or disabled in Control Panel's Device applet.

Effect: The parameters passed to the kernel-mode driver will not take effect.

Solution: Make sure that CSS-DVP.SYS and CSS-AVS.EXE are from the same release. Also check to make sure that CSS-DVP is neither stopped or disabled in Control Panel's Device applet.

Event ID=246

Message: Inactivity Scan of [Task Name] Started.

Cause:. This is an informational message indicating that a particular scanning task has started. Its purpose is to inform the user that the scan that starts after a specified period of inactivity (selected in the Schedule dialog box) has begun.

Effect: None.

Solution: None required.

Event ID=247

Message: Inactivity Scan of [Task Name] Completed.

Cause: This is an informational message indicating that a particular scanning task has finished. Its purpose is to inform the user that the scan that begins after a specified period of inactivity (selected in the Schedule dialog box) is now finished.

Effect: None.

Solution: None required.

Event ID=248

Message: [Task Name (command line parameter[s])] Scan Started

Cause: This is an informational message indicating that a scanning task was started from the command line. If the scanning task used any command-line parameters, those parameters will appear in the message.

Effect: None.

Solution: None required.

Event ID=249

Message: [Task Name] Scan Completed

Cause: This is an informational message indicating that a scanning task that was started from the command line has ended.

Effect: None.

Solution: None required.

Event ID=250

Message: An Error Occurred while Quarantining [Filename] into [Quarantine Directory].

Cause: The drive containing the quarantine directory may be full, preventing the process from taking place. A second cause could be that the service does not have read-write authority within that directory.

Effect: The file that was to be quarantined remains on the drive. As long as the file resides on the drive, there is a risk of further infection.

Solution: Check the amount of free disk space available. If the drive is full, free additional space so that infected files can be quarantined. Also, be sure that the service has read-write authority to the Quarantine directory.

Event ID=251

Message: While Scanning a File, AV Driver Reports [Filename]: Action =[Action taken on the Item Scanned], Result = [Optional Information on the Action Taken].

Cause: This is an informational message informing the user that a specific file has been successfully quarantined.

Effect: None.

Solution: None required.

Event ID=274

Message: While Scanning a File, AV Driver Reports: [Item Scanned] [Action Taken on the Item Scanned] Action=[Optional Information on Action Taken], Result=[File/Infection Information].

Cause: This is an informational message informing the user of which file was scanned and what action was taken on that file. Additionally, optional information regarding that action can be given. The final line in the message provides information on the nature of the infection.

Effect: None.

Solution: None required.

Event ID=276

Message: While Scanning Memory, AV Driver Reports: [Item Scanned] [Action Taken on the Item Scanned] Action=[Optional Information on Action Taken], Result=[File/Infection Information].

Cause: This is an informational message informing the user of the results of a memory scan. Information reported includes which memory item was scanned and what action was taken on that item. Additionally, optional information regarding that action can be given. The final line in the message provides information on the nature of the infection.

Effect: None.

Solution: None required.

Event ID=277

Message: While Scanning the Master Boot Record (MBR), AV Driver Reports: [Item Scanned] [Action Taken on the Item Scanned] Action=[Optional Information on Action Taken], Result=[File/Infection Information].

Cause: This is an informational message informing the user of the results of a MBR scan. Information reported includes the identity of the item scanned and what action was taken on that item. Additionally, optional information regarding that action can be given. The final line in the message provides information on the nature of the infection.

Effect: None.

Solution: None required.

Event ID=278

Message: While [Scanning an Item], AV Driver Reports: Action=[Action Taken on the Item Scanned], [Optional Information on Action Taken] Result=[File/Infection Information].

Cause: This is an informational message informing the user that the service has scanned a particular item (a file, memory, etc...) and is reporting what specific action was taken on that item. Optional information regarding the action can also be included. The final line provides information regarding the nature of the infection.

Effect: None.

Solution: None required.

Event ID=279

Message: While [Scanning an Item], AV Driver Reports: Action=[Action Taken on the Item Scanned], [Optional Information on Action Taken] Result=[File/Infection Information] within [Zip Filename].

Cause: This is an informational message informing the user that the service has scanned a particular zip-compressed file and is reporting what specific action was taken on that file. Optional information regarding the action can also be included. Also reported is the nature of the infection along with the name of the effected file.

Effect: None.

Solution: None required.

Event ID=280

Message: While [Scanning an Item], AV Driver Reports: Action=[Action taken on the Item Scanned], [Additional Information (when available)]   [Information on Action Taken] Result=[File/Infection Information].

Cause: This is an informational message informing the user that the service has scanned a particular item (a file, memory, etc...) and is reporting what specific action was taken on that item. Additional Information regarding the event is provided when available. Further, specific information regarding the action taken can also be included. The final line provides details regarding the nature of the infection.

Effect: None.

Solution: None required.

Event ID=281

Message: Task Statistics: [Number] Files Scanned [Number of Infected Files], [Number] of Zip Files [Number of Infected Zip Files] [Name of scanning task executed].

Cause: This is an informational message informing the user that the service has scanned files that previously were not scanned due either to system security or a setup error. The number of total files scanned is reported as is the number of zipped files scanned. Note that the number of zipped files scanned is included in the "Files Scanned" total. Additionally, the total number of infected files is reported as is the number of infected zipped files. The message also provides the name of the scanning task that was executed.

Effect: None.

Solution: None required.

Event ID=282

Message: AV Scheduler does not have the authority to Scan [Directory Name].

Cause: This is an informational message informing the user that Windows has denied the service access to a directory that was to be included in a scheduled scan.

Effect: The files located in the directory or directories mentioned in the message will not be scanned.

Solution: If you want to scan the directories, reconfigure the service so that it has access rights to those directories.

Event ID=283

Message: AV Scheduler Service could not switch to scanning account to [Account Name], [Error Description].

Cause: This is a message reporting a security/audit event. The service could not sign on using the account name specified in the error message. A description of the error follows the account name. Possible causes include a deleted account or a changed password. Additionally, the configuration settings within Command AntiVirus may have been updated with inaccurate or wrong information.

Effect: Scans that require the account's security privileges will not take place; typically, this will be a network drive/directory. However, it could also be a local drive or directory to which the service does not have access.

Solution: Check to see if the account has been deleted. If so, add it to the system again. If the account exists, check its password to make sure that it is correct. Likewise, make sure that the settings are accurate in Command AntiVirus Service Account dialog box.

Event ID=284

Message: AV Scheduler Service does not have the authority to access Task Directory [Directory Name].

Cause: Access information in Windows could be incorrect. Also, the server could be down or the access rights on the server could have changed. Another possible cause is that the security privileges of the account may have been changed. Similarly, the information in the Command AntiVirus Service Account dialog box may be incorrect.

Effect: No system tasks will be executed as scheduled scans.

Solution: Check the access information in Windows and make sure that the access settings are correct. Also, make sure that the server is not down, as could be the case when maintenance is being performed on the server. Additionally, check the security privileges of the account and change them accordingly if necessary. Another possible solution is to make sure that the Domain, Username and Password entries in the Command AntiVirus Service Account dialog box are accurate.

EVENT ID=285

Message: AV Scheduler Service switched to scanning account to [Account Name].

Cause: This is a informational security message indicating that the service successfully switched accounts to perform the requested scan. The message also indicates that the scheduler is scanning directories to which the default account (the local system account) does not necessarily have access.

Effect: None.

Solution: None needed.

EVENT ID=286

Message: F-Agent Requested an Inactivity Scan of [Task name].

Cause: This informational message is generated if detailed logging is enabled. The message indicates that F-Agent was monitoring for the system for certain types of inactivity (typically, mouse or keyboard inactivity). When the inactivity threshold was reached, F-Agent then requested the scheduler to perform a scan in the background.

Effect: None.

Solution: None needed.

EVENT ID=300

Message: Exception Occurred during Scheduling a Task.

Cause: This message was generated either by Command AntiVirus or Windows itself. As the task was being scheduled, an exception occurred. Rather than crashing, CSS AV Scheduler intercepted the exception/error and logged it accordingly.

Effect: The scheduled scanning task may not be launched. In rare cases, no further scheduled scans can take place. Unless corrected, the error could recur.

Solution: Report the error to Command Software Systems' Technical Support Department.

EVENT ID=301

Message: Exception Occurred while performing Scheduled or Inactivity Scan Task.

Cause: This message was generated either by Command AntiVirus or Windows itself. After the scheduled scan or the inactivity scan was launched, an exception occurred. The scan was unable to complete successfully. Rather than crashing, CSS AV Scheduler intercepted the exception/error and logged it accordingly. Unless corrected, the error could recur.

Effect: Some items that were supposed to be scanned were not scanned. Unless corrected, the error could recur.

Solution: Report the error to Command Software Systems' Technical Support Department.

EVENT ID=302

Message: Exception Occurred during Directory Traversal.

Cause: This message was generated either by Command AntiVirus or Windows itself. While scanning through directories specified in a scheduled scan task, an exception occurred. Rather than crashing, CSS AV Scheduler intercepted the exception/error and logged it accordingly.

Effect: Directories that were not scanned prior to the error will not be scanned for viruses. Unless corrected, the error could recur.

Solution: Report the error to Command Software Systems' Technical Support Department.

EVENT ID=303

Message: Exception Occurred while accessing a .ZIP file.

Cause: This message was generated either by Command AntiVirus or Windows itself. While attempting to access a zip-compressed file for scanning, an exception occurred. Rather than crashing, CSS AV Scheduler intercepted the exception/error and logged it accordingly.

Effect: The zip-compressed file may not have been successfully scanned for viruses. Unless corrected, the error could recur.

Solution: Report the error to Command Software Systems’ Technical Support Department.

EVENT ID=304

Message: Exception Occurred during Command Line Execution.

Cause: This message was generated either by Command AntiVirus or Windows itself. While attempting to run the scheduler from the command line, an exception occurred. Rather than crashing, CSS AV Scheduler intercepted the exception/error and logged it accordingly.

Effect: The scan that was requested from the command line was not completed either in whole or in part. Unless corrected, the error could recur.

Solution: Report the error to Command Software Systems’ Technical Support Department.

EVENT ID=305

Message: Exception Occurred during Service Scheduler Execution.

Cause: This message was generated either by Command AntiVirus or Windows itself. While attempting to execute the service scheduler, an exception occurred. Rather than crashing, CSS AV Scheduler intercepted the exception/error and logged it accordingly.

Effect: The service scheduler was not executed. Unless corrected, the error could recur.

Solution: Report the error to Command Software Systems’ Technical Support Department.

EVENT ID=306

Message: Exception Occurred during Service Scan Thread Execution.

Cause: This message was generated either by Command AntiVirus or Windows itself. While attempting to execute a service scanning thread (a scan started in its own thread or task space), an exception occurred. Rather than crashing, CSS AV Scheduler intercepted the exception/error and logged it accordingly.

Effect: All or part of the scheduled scan was not completed. Unless corrected, the error could recur.

Solution: Report the error to Command Software Systems' Technical Support Department.

MODIFYING LOG ENTRIES IN EVENT VIEWER

Within the Windows Event Viewer, the Application log collects events from CSS AV Scheduler. To modify the type of event items that are entered into the Application log, you can run the Windows Registry Editor (REGEDT32.EXE) and change the values accordingly.

The key in the registry containing the values is called DetailedLog. That key is located in the "HKEY_LOCAL_MACHINE\SOFTWARE\Command Software\F-PROT32\Preferences" path in the Windows registry. The default value for DetailedLog is "2".

The following list shows the available values that you can use in DetailedLog (Note: Use only the numerals as values. If you change a value, do not enter the text into the DetailedLog dialog box).

LogAlways	= 0
LogVirus	= 1
LogError	= 2
LogImportant	= 3
LogDetail	= 10

The reporting function of each numerical value is cumulative; that is, any given numeral contains the functions of all the lower numerals that precede it. So, the higher the numeral, the greater its reporting ability. For example, a value of “2” will write LogError, LogVirus and LogAlways messages to the Application log in Event Viewer. As a second example, a value of “10” will write the LogDetail, LogImportant, LogError, LogVirus, and LogAlways messages to the Application log. As the DetailedLog values are cumulative, only a single numerical value at a time can be used in DetailedLog.

INDEX