

Command AntiVirus™

for

Windows®

Microsoft® Windows® 95, 98, Me, NT®, 2000, and XP

User'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.**

**Command AntiVirus © Copyright 2003 by Command Software Systems, Inc.
Portions © Copyright 1993, 2003 FRISK Software International.**

Published in the U.S.A. by Command Software Systems, Inc. All rights reserved.
Document No. CW32U-480-0303

Part No. 07-9200-00

TABLE OF CONTENTS

INTRODUCTION	1-1
Main Features	1-1
Chapter Overview	1-2
Chapter 1 - Introduction	1-2
Chapter 2 - Installation	1-2
Chapter 3 - Using Command AntiVirus	1-2
Chapter 4 - Boot Record Support	1-3
Chapter 5 - DOS Recovery	1-3
Chapter 6 - Glossary	1-3
Conventions Used	1-4
System Requirements	1-6
Testing Command AntiVirus	1-7
Additional Information	1-8
Web Site	1-8
Help	1-8
Mailing List Server	1-8
Readme.txt	1-9
INSTALLATION	2-1
System Requirements	2-2
Installing	2-3
Typical Installation	2-4
Custom Installation	2-9
Creating and Using a Rescue Disk Set	2-19
Creating From the Rescue Disks Menu	2-19
Using the Rescue Disk Set	2-23
Installation Maintenance	2-24
Starting the Installation Maintenance Program	2-25
Adding or Removing Features	2-27
Repairing the CSAV Installation	2-29
Removing Command AntiVirus	2-30
USING COMMAND ANTIVIRUS	3-1
The CSAV Main Dialog Box	3-3
Task Window	3-5
Command Buttons	3-10
Shortcut Menu	3-12
Menu Bar	3-12
Toolbar Buttons	3-19
Other Ways to Access Command AntiVirus	3-19
Creating and Using a Rescue Disk Set	3-20

Creating From the Rescue Disks Menu	3-21
Using the Rescue Disk Set	3-24
Starting an On-demand Scan	3-25
From the Task Menu	3-26
From the Windows Shortcut Menu	3-33
From the Command Line	3-34
Scheduling an On-demand Scan	3-35
Understanding On-access Scan Reporting	3-39
Viewing Scan Results	3-40
From the View Menu	3-41
In the Windows Event Viewer	3-45
Customizing Scan Results Reporting	3-49
Setting a Virus Definition Files Warning	3-52
Updating Command AntiVirus	3-55
Checking for Updates On-demand	3-55
Checking for Updates Automatically	3-61
Creating a New Scan Task	3-76
Setting Scan Task Properties	3-78
Copying a Scan Task	3-85
Deleting a Scan Task	3-88
Setting On-access Scanning Properties	3-89
Specifying Files/Directories To Scan	3-93
Adding Additional File Types to Scan	3-94
Specifying Files to Exclude From Scans	3-97
Specifying Directories to Exclude From Scans	3-99
Using the Quarantine Feature	3-102
Sending a Virus Notification Message	3-110
Setting Up Virus Reporting to a NetWare Server	3-112
Setting CSAV Scanning Options for NetWare Drives	3-115
Changing the System Scan Task Folder	3-118
Scanning Mail	3-121
Getting Help	3-123
Finding Information on a Specific Topic	3-124
Finding Information on the Latest Changes	3-124
Contacting a Technical Support Representative	3-125
Viewing a List of Viruses Handled by CSAV	3-125
Viewing CSAV Product Installation Information	3-125

BOOT RECORD SUPPORT	4-1
FIXDSKNT.EXE	4-1
Using FIXDSKNT to Create a Rescue File	4-1
FIXDISK Command-line Options	4-3
Disinfecting a Boot Sector Virus	4-5
If Disinfecting Fails	4-7
DOS RECOVERY	5-1
F-PROT.EXE Menu Options	5-2
Scan	5-3
Options	5-10
Information	5-12
Quit	5-13
Command-line Mode	5-14
F-PROT.EXE Return Codes	5-17
GLOSSARY	6-1
INDEX	I-1

INTRODUCTION

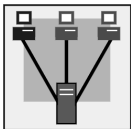


This chapter provides an overview of Command AntiVirus for Windows® including a list of product features, system requirements, and conventions used throughout this user's guide. It also contains details on accessing additional product-related information from the Command Software Systems web site.

MAIN FEATURES

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

- A Windows NT® compliant 32-bit scanner and a kernel-mode driver with support for long file names and Universal Naming Convention (UNC) path names.
 - On-access scanning of files and disks as they are accessed. This on-access protection is referred to as Dynamic Virus Protection.
 - Right mouse support that allows you to easily start a scan on any file or folder.
 - The ability to schedule scans to run in the background on local drives on a specific day, week, or month.
 - The ability to add or delete files and folders from the scan list.
 - Scanning of compressed files and compressed executables.
 - Safe removal of viruses from files, boot sectors, and partition tables.
 - The ability to isolate virus infections to a quarantine folder automatically.
 - The ability to check for updates and/or upgrades automatically.
-



- The ability to scan messages and attachments of incoming and outgoing mail for viruses sent through Microsoft Outlook®.
- In Windows NT/2000/XP, the ability to create separate administrative and user-defined scan tasks.
- The ability to e-mail a virus infection report to multiple recipients.
- ICSA certification for effective virus protection.

CHAPTER OVERVIEW

The *Command AntiVirus for Windows® User's Guide* consists of the following chapters:

CHAPTER 1 - INTRODUCTION

This chapter provides an overview of the product including a list of features, system requirements, and conventions used throughout this guide. 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 and using a rescue disk set, adding and removing features, and reinstalling and removing Command AntiVirus.

CHAPTER 3 - USING COMMAND ANTIVIRUS

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

For example, Chapter 3 includes step-by-step instructions on starting, scheduling, creating, and customizing virus scan tasks. It also contains information on viewing scan results, updating Command AntiVirus, and customizing on-access scanning.

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 - GLOSSARY

The *Glossary* provides definitions of virus terminology.

CONVENTIONS USED



Indicates an area that requires special attention.



Indicates a helpful tip.



Indicates information that is specific to Windows NT.



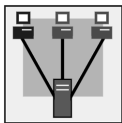
Indicates information that is specific to Windows 2000/XP.



Indicates information that is specific to Windows NT/2000/XP.



Indicates information that is specific to Windows 95/98/Me.



Indicates network-specific information.

COURIER Examples and messages appear in COURIER. For example:

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

CSAV The acronym used for Command AntiVirus.

Italics A reference to the manual is in italics.

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

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

SYSTEM REQUIREMENTS

To install and operate Command AntiVirus for Windows, you **must** have at least **one** of the following Microsoft® Windows 32-bit platforms installed:

- Windows XP Home
- Windows XP Professional
- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows NT® 4.0 with Service Pack 4 or higher
- Windows NT® Server edition 4.0 with Service Pack 4 or higher
- Windows Me
- Windows 98
- Windows 98 SE
- Windows 95 OSR2

You **must** also have Microsoft Internet Explorer 5.0 or higher installed.

If you are running Windows 95 OSR2, you **must** also have the Command AntiVirus Pre-installation Convenience Pack installed. You can download this package from our web site at:

<http://www.commandsoftware.com/downloads/commercial/csavpc.cfm>

TESTING COMMAND ANTIVIRUS

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

If you run this file, you will find a test file called **EICAR.COM** (from the European Institute for Computer Anti-Virus Research). This file helps you verify that you installed your anti-virus protection properly and that DVP on-access protection is working. **EICAR.COM** lets you create and safely test customized virus warning messages. It also provides a way to demonstrate how Command AntiVirus responds when it finds a virus.

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

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

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

If DVP **is** active when you run **EICAR.COM**, the system displays the **Command AntiVirus for Windows – Dynamic Virus Protection Report** log. This log provides the details for **all** virus infections found.

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:

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

HELP

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

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

MAILING LIST SERVER

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

README.TXT

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



INSTALLATION

You can install Command AntiVirus (CSAV) for Windows® quickly and easily using the **Typical** installation, or you can choose the components that you want to install by selecting the **Custom** installation.

This chapter contains information that will help you to:

- Install Command AntiVirus on a single workstation or server
- Create and use a recovery Rescue Disk set
- Add or remove features after installation
- Repair the Command AntiVirus installation
- Remove Command AntiVirus

We suggest that you read through the installation 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.



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

SYSTEM REQUIREMENTS

To install and operate Command AntiVirus for Windows, you **must** have at least **one** of the following Microsoft® Windows 32-bit platforms installed:

- Windows XP Home
- Windows XP Professional
- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows NT® 4.0 with Service Pack 4 or higher
- Windows NT® Server edition 4.0 with Service Pack 4 or higher
- Windows Me
- Windows 98
- Windows 98 SE
- Windows 95 OSR2

You **must** also have Microsoft Internet Explorer 5.0 or higher installed.

If you are running Windows 95 OSR2, you **must** also have the Command AntiVirus Pre-installation Convenience Pack installed. You can download this package from our web site at:

<http://www.commandsoftware.com/downloads/commercial/csavpc.cfm>

INSTALLING

During the Command AntiVirus installation, you can choose a **Typical** or a **Custom** installation.

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

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



The Command AntiVirus installation is in Microsoft Installer (**.MSI**) package format. For machines that do not have the Windows Installer, the installation **SETUP.EXE** installs the Windows Installer and then launches the **.MSI**.



After the installation of the Windows Installer, it may be necessary to restart your computer.



To install Command AntiVirus on Windows NT, Windows 2000, or Windows XP, you **must** be a member of the Administrators group on the local machine.

As Windows Installer 1.1 requires the original media to install Command AntiVirus virus definition files and component updates, we highly recommend that you:

- Create a folder on your local hard drive
- Copy the installation files to that folder
- Install CSAV from your local hard drive
- Do **not** remove the folder from your local hard drive

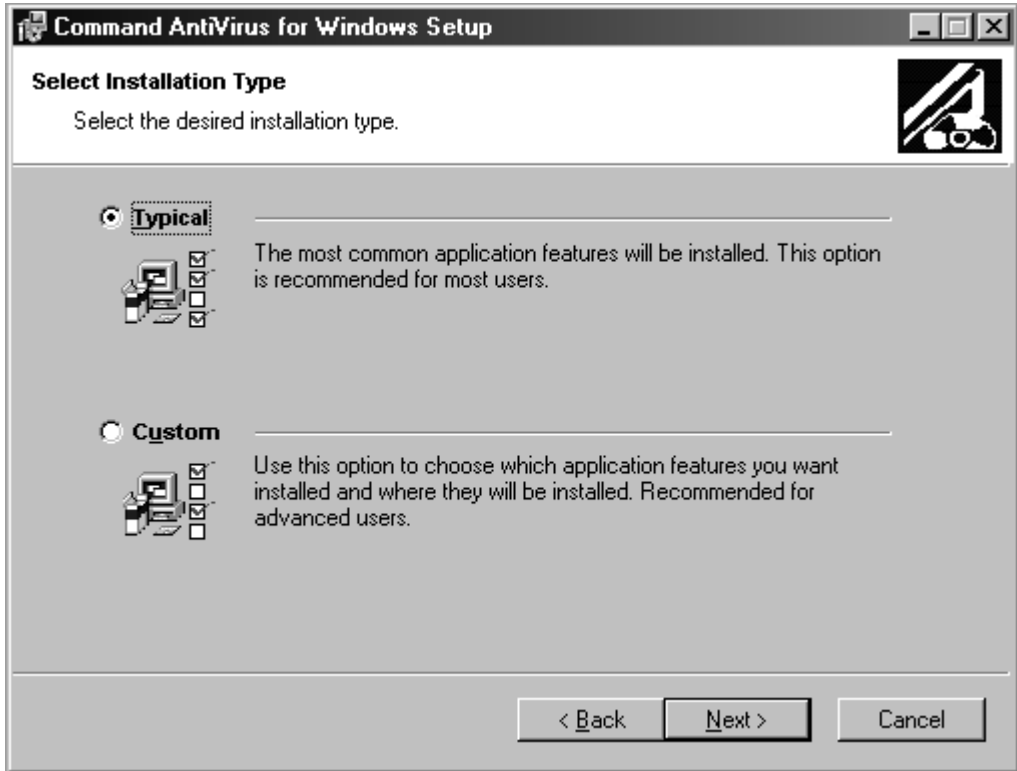


This section contains information on how to install Command AntiVirus for Windows using the **Typical** or the **Custom** installation.

TYPICAL INSTALLATION

To install Command AntiVirus, follow these steps:

1. Create a folder on your local hard drive, for example, **CSAVMSI**.
2. Copy the CSAV installation files into the folder that you created in **Step 1**.
 - **If you have downloaded CSAV** – Copy and extract the downloaded self-extracting file.
 - **If you have a CD** – Browse the CD to search for the **Win32** folder. Open the folder, and copy the files.
3. Open the folder that you created in **Step 1**.
4. Double-click **SETUP.EXE**. The system displays the **Welcome** dialog box.
5. Click **Next**. The system displays the **README** file that contains the latest product information.
6. Click **Next**. The system displays the **License Agreement**.
7. To accept the license agreement, select **I accept the license agreement**, and click **Next**. The system displays the **Select Installation Type** dialog box:



Select Installation Type Dialog Box

8. 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.

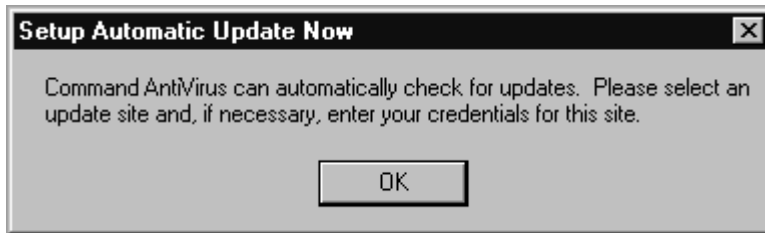


NOTE: You can click **Cancel**, **Exit Setup**, and then **OK** to cancel the installation and exit the setup program.

When the copying is complete, the system displays the **Setup Automatic Update Now** dialog box.

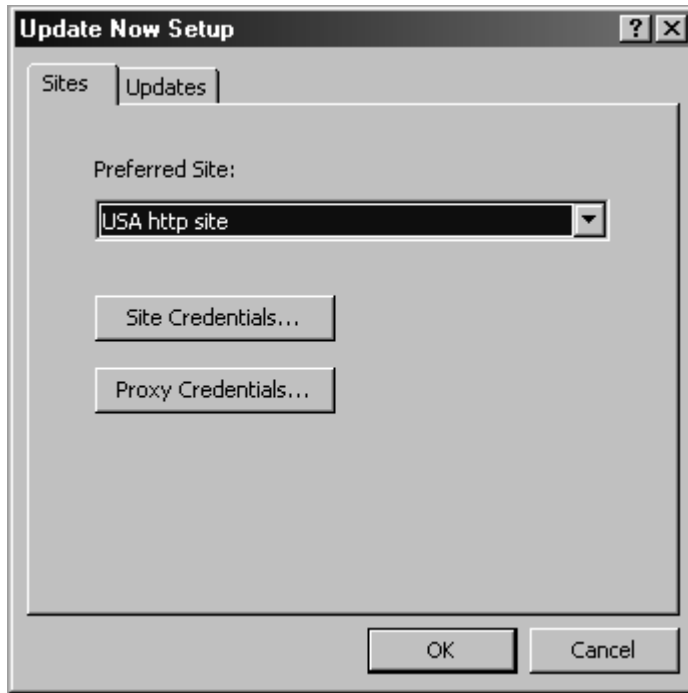


NOTE: If you are reinstalling Command AntiVirus and you kept your customized **Preferences/Update Now** settings, the system displays a dialog box informing you that Command AntiVirus for Windows has been successfully installed. Go to **Step 17**.



Setup Automatic Update Now Dialog Box

9. Click **OK**. The system displays the **Update Now** dialog box with the **Sites** dialog box in view:



Sites Dialog Box


10. Under **Preferred Site**, click the drop-down arrow, and select a site for which you are authorized, for example, **USA http site**.
11. Click the **Site Credentials** button. The system displays the **Enter Network Password** dialog box:

A screenshot of a Windows dialog box titled "Enter Network Password". The dialog box has a standard Windows window border with a close button (X) in the top right corner. On the left side, there is a key icon. The main text reads "Please type your user name and password." Below this, the "Site:" is listed as "http://download.commandsoftware.com/". There are two text input fields: "User Name" and "Password". At the bottom, there are two buttons: "OK" and "Cancel".

Enter Network Password Dialog Box

12. In the **User Name** text box, type your Command user name.
13. In the **Password** text box, type your Command password.
14. Click **OK**. The system returns to the **Sites** dialog box.
15. If you do **not** use a proxy server, go to **Step 16**.
If you do use a proxy server, click the **Proxy Credentials** button and repeat **Steps 12** through **14**.
16. Click **OK**. The system displays a dialog box informing you that Command AntiVirus for Windows has been successfully installed.

Command AntiVirus is now set to check for updates and/or upgrades automatically and to notify you that new files are available.

When new files are available, the system displays a **Download available** notification icon  in the Windows notification area.

For information on what to do when a notification icon is displayed in the Windows notification area, refer to **Understanding the Notification Messages** located in the *Using Command AntiVirus* chapter of this guide.

For information on additional notification and download options, refer to **Setting Up the Notification Process** in the *Using Command AntiVirus* chapter of this guide.

17. Click **Finish** to exit.

You can now open the Command AntiVirus graphical user interface (GUI) by double-clicking the Command AntiVirus notification icon (yellow **C**) located in the Windows notification area to the right of the Quick Launch bar.



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

For more information on updating your virus definition files, refer to **Updating Command AntiVirus** located in the *Using Command AntiVirus* chapter of this guide.

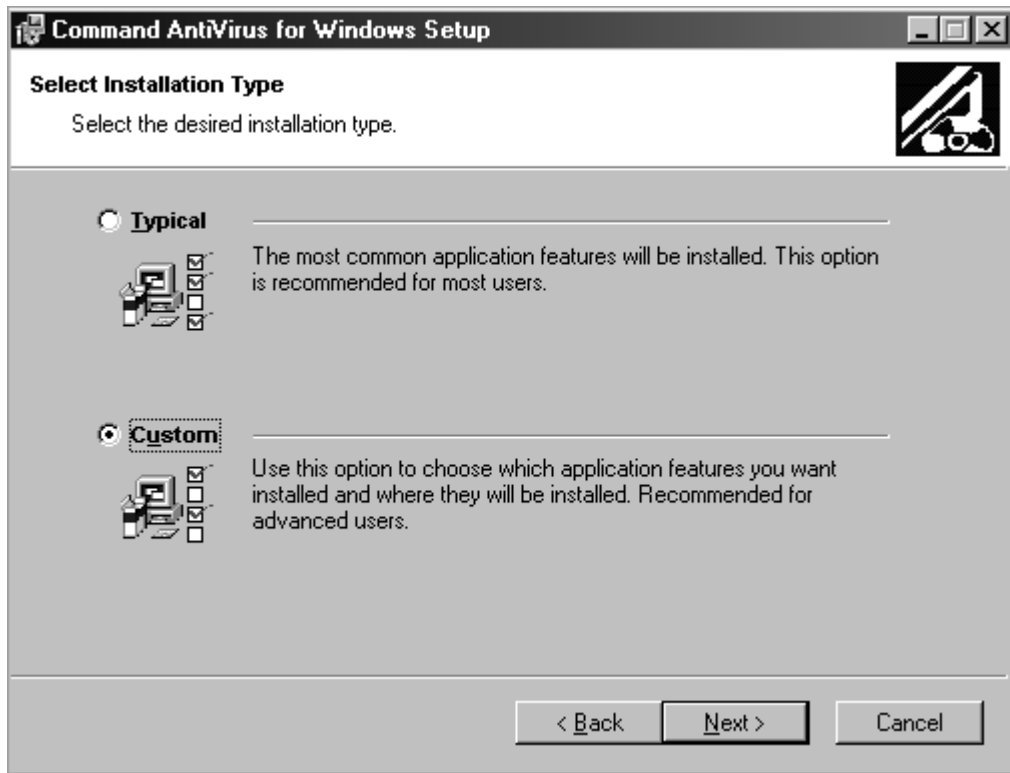


NOTE: We highly recommend that you create a Rescue Disk set from the **Rescue Disk** menu in the Command AntiVirus graphical user interface (GUI). For more information, refer to **Creating and Using a Rescue Disk Set** located later in this chapter.

CUSTOM INSTALLATION

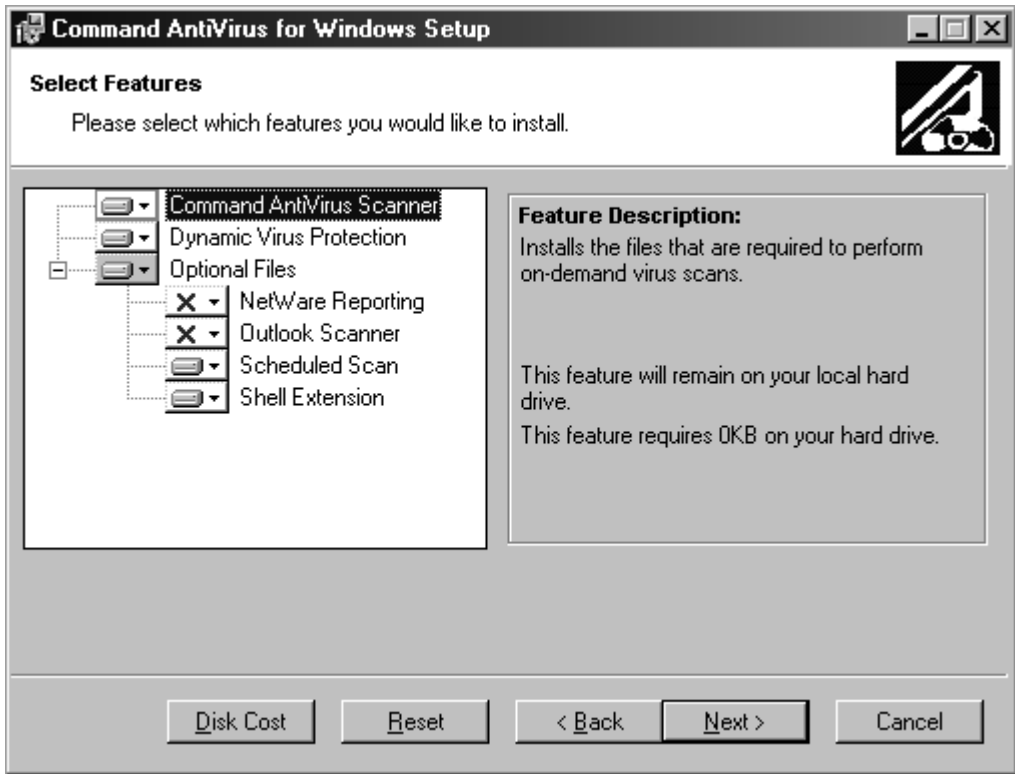
1. Create a folder on your local hard drive, for example, **CSAVMSI**.
2. Copy the CSAV installation files into the folder that you created in **Step 1**.
 - **If you have downloaded CSAV** – Copy and extract the downloaded self-extracting file.
 - **If you have a CD** – Browse the CD to search for the **Win32** folder. Open the folder, and copy the files.
3. Open the folder that you created in **Step 1**.

4. Double-click **SETUP.EXE**. The system displays the **Welcome** dialog box.
5. Click **Next**. The system displays the **README** file that contains the latest product information.
6. Click **Next**. The system displays the **License Agreement**.
7. To accept the license agreement, select **I accept the license agreement**, and click **Next**. The system displays the **Select Installation Type** dialog box:



Select Installation Type Dialog Box

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



Select Features Dialog Box

9. 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.
 - **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:

- **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.

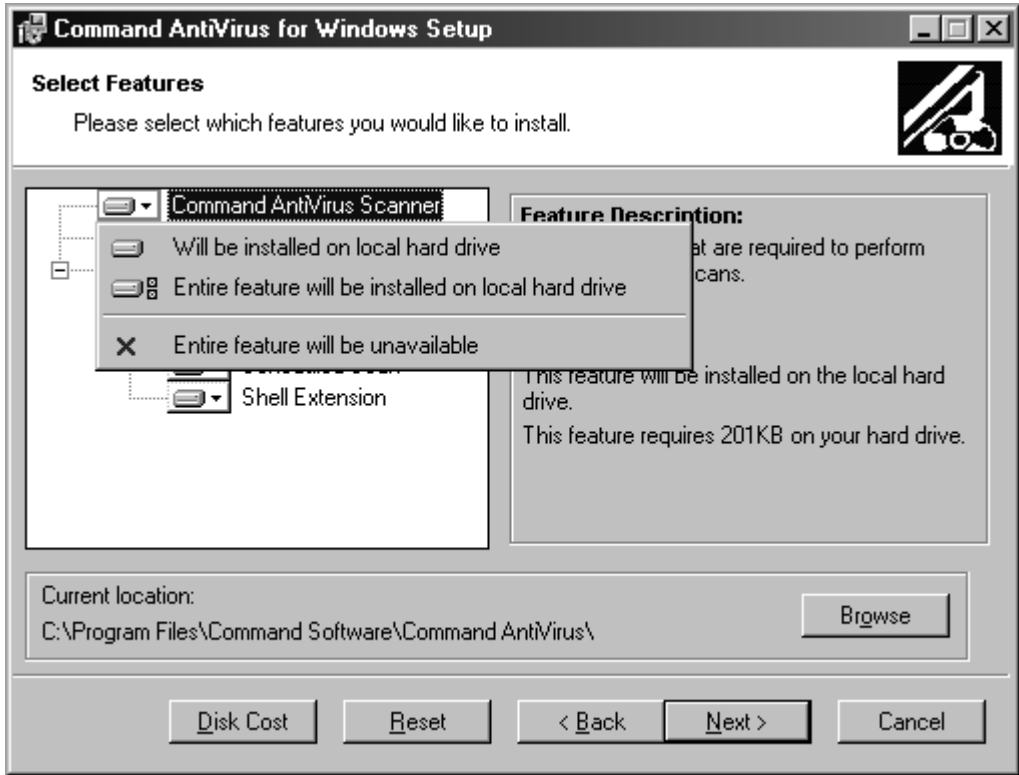
- **Outlook Scanner** – installs the files that are required to perform on-access virus scans of incoming and outgoing mail in Microsoft Outlook®. This subfeature is **not** installed by default.



NOTE: The Outlook Scanner does **not** apply to Microsoft Outlook Express.

- **Scheduled Scan** – installs the files that are required to perform scheduled virus scans. This subfeature is installed by default.
- **Shell Extension** – installs the files that are required to add the Command AntiVirus scan option to the shell shortcut menu. 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 drop-down arrow  located to the right of the icon. The system displays a drop-down menu:



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 **Scheduled Scan, Optional Files** 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 **Optional Files, Netware Reporting, Outlook Scanner, Scheduled Scan, Shell Extension, and Update Now** 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.



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\Command AntiVirus\`. To select a different folder, use the **Browse** button.



NOTE: You can change only the location of files that are unique to Command AntiVirus for Windows. Files that are shared among other Command AntiVirus products such as the virus definition files are automatically stored in the operating 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**.

- 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 **Configure Automatic Update Now** dialog box.

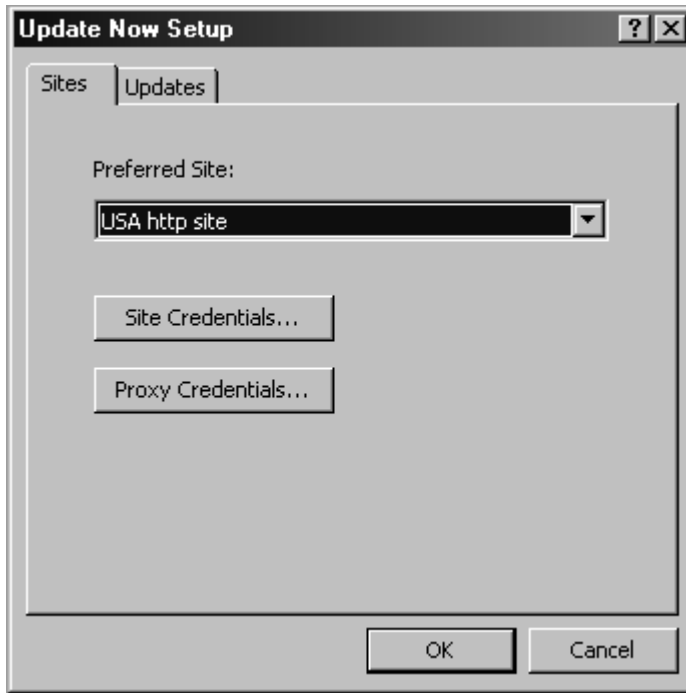


NOTE: If you are reinstalling Command AntiVirus and you kept your customized **Preferences/Update Now** settings, the system displays a dialog box informing you that Command AntiVirus for Windows has been successfully installed. Go to **Step 19**.



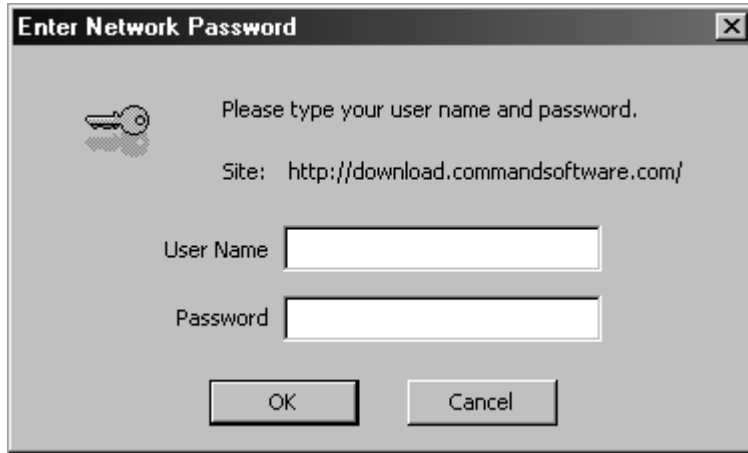
Configure Automatic Update Now Dialog Box

- Click **OK**. The system displays the **Update Now** dialog box with the **Sites** dialog box in view:



Sites Dialog Box


12. Under **Preferred Site**, click the drop-down arrow, and select a site for which you are authorized, for example, **USA http site**.
13. Click the **Site Credentials** button. The system displays the **Enter Network Password** dialog box:



Enter Network Password Dialog Box

14. In the **User Name** text box, type your Command user name.
15. In the **Password** text box, type your Command password.
16. Click **OK**. The system returns to the **Sites** dialog box.
17. If you do **not** use a proxy server, go to **Step 18**.
If you do use a proxy server, click the **Proxy Credentials** button, and repeat **Steps 14** through **16**.
18. Click **OK**. The system displays a dialog box informing you that Command AntiVirus for Windows has been successfully installed.

Command AntiVirus is now set to check for updates and/or upgrades automatically and to notify you that new files are available.

When new files are available, the system displays a **Download available** notification icon  in the Windows notification area.

For information on what to do when a notification icon is displayed in the Windows notification area, refer to **Understanding the Notification Messages** located in the *Using Command AntiVirus* chapter of this guide.

For information on additional notification and download options, refer to **Setting Up the Notification Process** in the *Using Command AntiVirus* chapter of this guide.

19. Click **Finish** to exit.

You can now open the Command AntiVirus graphical user interface (GUI) by double-clicking the Command AntiVirus notification icon (yellow **C**) located in the Windows notification area to the right of the Quick Launch bar.



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

For more information on updating your virus definition files, refer to **Updating Command AntiVirus** located in the *Using Command AntiVirus* chapter of this guide.



NOTE: We highly recommend that you create a Rescue Disk set from the **Rescue Disk** menu in the Command AntiVirus graphical user interface (GUI). For more information, refer to **Creating and Using a Rescue Disk Set** located later in this chapter.

CREATING AND USING A RESCUE DISK SET

Some viruses may prevent you from starting up your system or accessing your Command AntiVirus program. A **Rescue Disk** set helps you to detect and remove these viruses.

The **Rescue Disks** menu in the Command AntiVirus graphical user interface (GUI) allows you to create a **Rescue Disk** set. You can access this menu by clicking **Rescue Disks** 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.

This section contains information on how to create a **Rescue Disk** set from the Command AntiVirus **Rescue Disks** menu and how to use the **Rescue Disk** set when you cannot use your Command AntiVirus program.

CREATING FROM THE RESCUE DISKS MENU

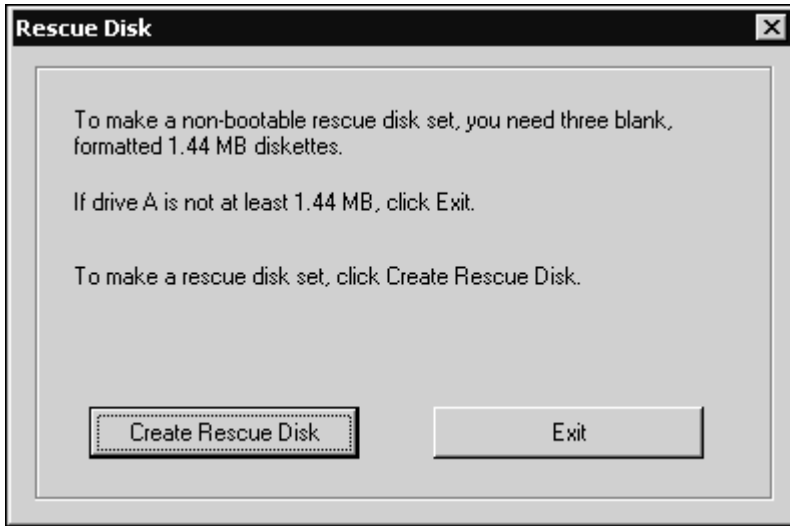
To create a **Rescue Disk** set from the **Rescue Disks** menu, follow these steps:

1. Open the Command AntiVirus graphical user interface (GUI).
2. On the menu bar, click **Rescue Disks**. The system displays the **Rescue Disks** menu:



Rescue Disks Menu

3. Click **Make Rescue Disks**, the system displays the **Rescue Disk** dialog box:

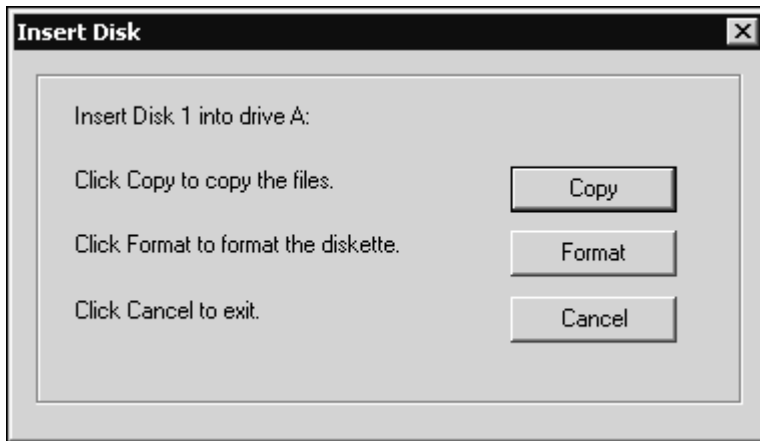


Rescue Disk Dialog Box



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

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



Insert Disk Dialog Box

5. Insert **Disk 1** into drive A, and click **Copy**. The system displays the **Copying** dialog box that shows the files being copied.

When the copying is complete, the system returns to the **Insert Disk** dialog box which prompts you for **Disk 2**.



NOTE: If your disk is **not** formatted, insert **Disk 1**, and click **Format**. Then, continue with the formatting process. When the formatting process is complete, click **Close** to return to 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 displays the **Copying** dialog box that shows the files being copied.

When the copying is complete, the system returns to the **Insert Disk** dialog box which prompts you for **Disk 3**.

8. Remove **Disk 2** from drive A, and set the write-protect tab to prevent any modifications.
9. Insert **Disk 3** into drive A, and click **Copy**. The system displays the **Copying** dialog box that shows the files being copied.

When the copying is complete, the system returns to the **Command AntiVirus Main** dialog box.

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

If necessary, you can run a Command AntiVirus scan from the **Rescue Disk** set.

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



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

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

USING THE RESCUE DISK SET

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

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

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

6. At the A prompt, type the following:

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

7. Press **Enter**. The system prompts you to insert a diskette with **SIGN.DEF**.

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

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

When the scan is complete, remove **Rescue Disk 3** from drive A.

INSTALLATION MAINTENANCE

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



In Windows NT, Windows 2000, or Windows XP, to perform any of the installation maintenance tasks, you **must** be a member of the Administrators group on the local machine.

This section contains information on how to:

- Start the installation maintenance program
- Add or remove features
- Repair the Command AntiVirus installation
- Remove Command AntiVirus

STARTING THE INSTALLATION MAINTENANCE PROGRAM

To start the installation maintenance program, follow these steps:

1. On the Windows taskbar, click the **Start** button.
2. Select **Settings**, and click **Control Panel**.
3. Double-click **Add/Remove Programs**. The system displays the **Add/Remove Programs** dialog box.
4. Select **Command AntiVirus for Windows** from the list of currently installed programs, and click the **Add/Remove** or the **Change** button. The system displays the Command AntiVirus installation program's **Application Maintenance** dialog box:



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

For more information on **Adding or Removing Features, Repairing the CSAV Installation, and Removing Command AntiVirus**, refer to the corresponding topic located later in this section.

ADDING OR REMOVING FEATURES

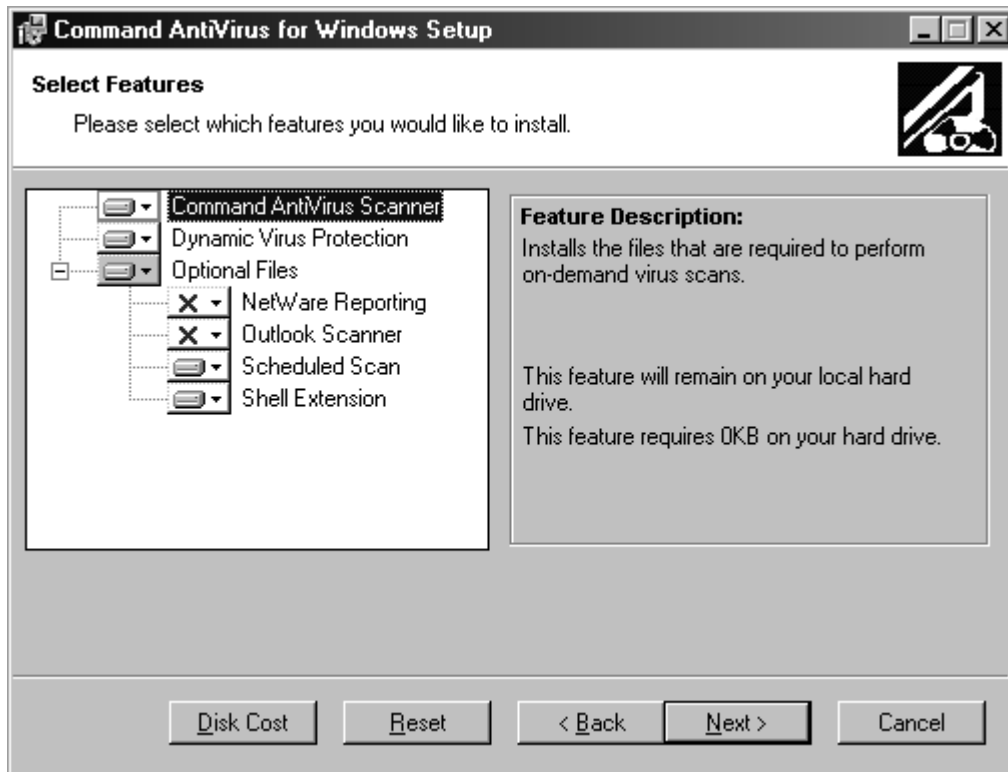
After you have installed Command AntiVirus for Windows, you can add or remove features through the installation program's **Application Maintenance** dialog box.



In Windows NT, Windows 2000, or Windows XP, to add or remove features, you **must** be a member of the Administrators group on the local machine.


To add or remove features, follow these steps:

1. On the Windows taskbar, click the **Start** button.
2. Select **Settings**, and click **Control Panel**.
3. Double-click **Add/Remove Programs**. The system displays the **Add/Remove Programs** dialog box.
4. Select **Command AntiVirus for Windows** from the list of currently installed programs, and click the **Add/Remove** or the **Change** button. The system displays the Command AntiVirus installation program's **Application Maintenance** dialog box.
5. Select **Modify**, and click **Next**. The system displays the **Select Features** dialog box:



Select Features Dialog Box

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

To select a different installation state, click the drop-down arrow  located 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**.

- 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.

When the updating is complete, the system displays a dialog box informing you that Command AntiVirus for Windows has been successfully installed.

- Click **Finish** to exit.

REPAIRING THE CSAV INSTALLATION

You can repair the Command AntiVirus for Windows installation through the installation program's **Application Maintenance** dialog box. This option allows you to reinstall missing or corrupt files, registry keys, and shortcuts.



In Windows NT, Windows 2000, or Windows XP, to repair the Command AntiVirus installation, you **must** be a member of the Administrators group on the local machine.

To repair the Command AntiVirus installation, follow these steps:

- On the Windows taskbar, click the **Start** button.
- Select **Settings**, and click **Control Panel**.
- Double-click **Add/Remove Programs**. The system displays the **Add/Remove Programs** dialog box.
- Select **Command AntiVirus for Windows** from the list of currently installed programs, and click the **Add/Remove** or the **Change** button. The system displays the Command AntiVirus installation program's **Application Maintenance** dialog box.

5. 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.

6. 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.

When the copying is complete, the system displays a dialog box informing you that Command AntiVirus for Windows has been successfully installed.

7. Click **Finish** to exit.

REMOVING COMMAND ANTIVIRUS

You can completely remove an installed version of Command AntiVirus for Windows through the installation program's **Application Maintenance** dialog box.



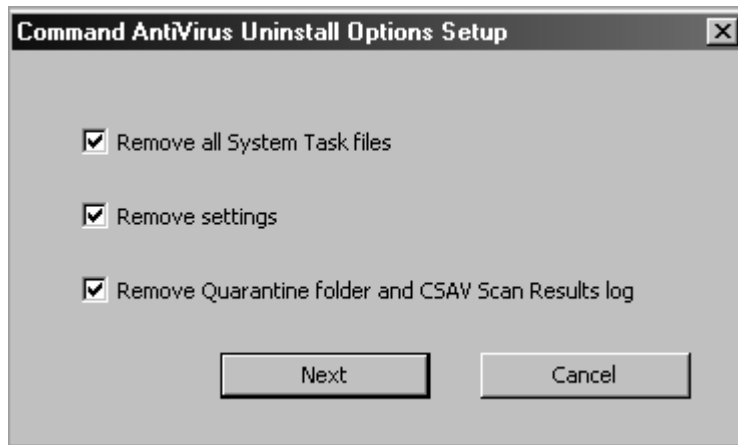
In Windows 2000 and Windows XP, you can also remove Command AntiVirus by clicking the **Remove** button in the Windows **Add/Remove Programs** dialog box.



In Windows NT, Windows 2000, or Windows XP, to remove Command AntiVirus, you **must** be a member of the Administrators group on the local machine.

To remove Command AntiVirus completely, follow these steps:

1. On the Windows taskbar, click the **Start** button.
2. Select **Settings**, and click **Control Panel**.
3. Double-click **Add/Remove Programs**. The system displays the **Add/Remove Programs** dialog box.
4. Select **Command AntiVirus for Windows** from the list of currently installed programs, and click the **Add/Remove** or the **Change** button. The system displays the Command AntiVirus installation program's **Application Maintenance** dialog box.
5. Select **Remove**, and click **Next**. The system displays the **Uninstall** dialog box.
6. Click **Next**. The system displays the **Command AntiVirus Uninstall Options Setup** dialog box:



CSAV Uninstall Options Setup Dialog Box

This dialog box allows you to remove or keep **all** of your **System Task** files, **all** of your customized **Preferences** settings, and/or the current **Quarantine** folder and the **CSAV Scan Results** log. The options are selected by default to delete **all** of the files.

7. Select or clear the following options:

- **Remove all System Task files** – Deletes all of the **System Task** files listed in the Command AntiVirus **Task List**.
- **Remove settings** – Deletes all of your customized **Preferences** settings. These are the options that you set from the Command AntiVirus **Preferences** menu, for example, your customized virus infection **Reporting** options.
- **Remove Quarantine folder and CSAV Scan Results log** – Deletes the current **Quarantine** folder and the **Command AntiVirus Scan Results** log.



NOTE: The current **Quarantine** folder is removed only if the folder is on the local drive. If the current **Quarantine** folder is on a network drive, it is not removed.

8. 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.

When the removal is complete, the system displays a dialog box informing you that Command AntiVirus for Windows has been successfully uninstalled.

9. Click **Finish** to exit.

USING COMMAND ANTIVIRUS



Command AntiVirus for Windows® is easy to use. You can keep your system virus free quickly and easily by using the Command AntiVirus preset scan tasks and settings, or you can customize scan tasks and settings to fit your particular needs.

Through its on-access, on-demand, and mail scanning features, Command AntiVirus (CSAV) for Windows provides an effective and easy way to scan for viruses:

- **On-access Scanning** – Protects your system from becoming infected between full scans. This on-access, “behind-the-scenes” protection is provided through Dynamic Virus Protection (DVP). DVP runs transparent, on-access scans of each program that is run or file that is opened.

DVP is turned on by default and is set to disinfect when a virus infection is found. You can turn off DVP protection or change its on-access scanning properties through the **Preferences** menu of the **Command AntiVirus Main** dialog box. For more information, refer to **Setting On-access Scanning Properties** located later in this chapter.

- **On-demand Scanning** – Command AntiVirus comes with several preconfigured scan tasks that allow you to perform a full scan of your diskette drives, local hard drives, network drives, or CD-ROM drives.

By default, these scan tasks are set to disinfect when a virus infection is found. You can change the scanning properties of a scan task, create a new scan task, or schedule when you want an on-demand scan to take place through the **Task** menu of the **Command AntiVirus Main** dialog box. For more information, refer to **Setting Scan Task Properties** and **Scheduling an On-demand Scan** located later in this chapter.

- **Mail Scanning** – Command AntiVirus includes a plugin for Microsoft Outlook® called the Outlook Scanner. The Outlook Scanner scans messages and attachments of incoming and outgoing mail for viruses. Unscanned mail is scanned and marked as scanned when it is opened. For more information, refer to **Scanning Mail** located later in this chapter.

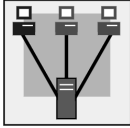


NOTE: The Outlook Scanner does **not** apply to Microsoft Outlook Express.

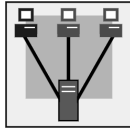
The Outlook Scanner is **not** installed by default. This feature must be installed during installation or afterwards by using the installation program's **Application Maintenance** dialog box. For more information on installation, refer the **Installation** chapter of this guide.

This chapter contains information that will help you to:

- Become familiar with the **Command AntiVirus Main** dialog box
- Create and use a recovery Rescue Disk Set
- Start or schedule an on-demand scan
- Understand what happens when a virus infection is found through on-access scanning
- View scan results
- Customize how and where scan results are reported
- Set up displaying a warning message when the virus definition files are out-of-date
- Update Command AntiVirus
- Create, copy or delete a scan task
- Set the properties of a scan task
- Set the properties of on-access scanning
- Specify additional file types to include in and what files and/or directories to exclude from all scans



- Use the Quarantine feature
- Set up e-mailing a virus notification message when a virus infection is found
- Set up virus reporting to a NetWare® server

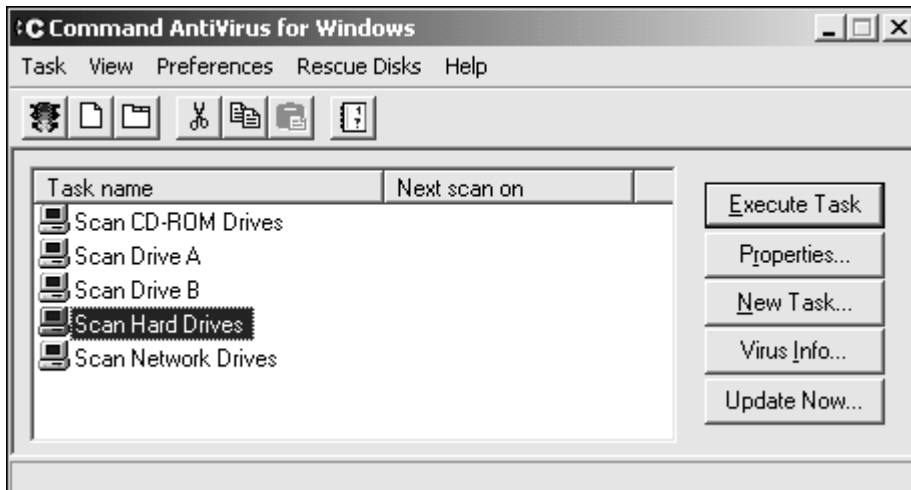


- Set how CSAV behaves when scanning a network drive that has NetWare installed
- Change the folder that contains the **System** Scan Tasks
- Scan mail
- Get help

THE CSAV MAIN DIALOG BOX

Command AntiVirus uses a graphical user interface (GUI) that allows you to start, schedule, and customize on-demand scan tasks quickly and easily. From the GUI, you can also start or stop on-access scanning, set the on-access scanning properties, and customize how Command AntiVirus behaves. For example, you can set Command AntiVirus to send a warning message when your virus definition files are out-of-date.

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 start, schedule, create, delete, and modify a virus scan task.

You can perform these scan-task operations through the easy-to-use options found in the menu bar, toolbar, command buttons, and keyboard shortcuts. Just use the **Task List** to select a specific 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 create scan tasks, view scan results, set up Command AntiVirus, create a Rescue Disk set, or find help.

This section contains information on the items that make up the **Command AntiVirus Main** dialog box:

- Task Window
- Command Buttons
- Shortcut Menu
- Menu Bar
- Toolbar Buttons
- CSAV Icon
- Command AntiVirus Shortcut Menu

TASK WINDOW

The main feature in the **Command AntiVirus Main** dialog box is the **Task Window**. This window contains a **Task List** that contains two column headers: **Task name** and **Next scan on**.

The **Task name** column contains a list of small icons with the scan task name located to the right of each icon. The **Next Scan On** column shows the time of the next scheduled on-demand scan.

From the **Task List**, you can create, set up, 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	Next scan on
Scan CD-ROM Drives	
Scan Drive A	
Scan Drive B	
Scan Hard Drives	
Scan Network Drives	

Task List View

Column header Split bar

Command AntiVirus comes with several preset scan 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 scan task name.



Types of Scan Tasks



In Windows 95, Windows 98, and Windows Me, the preset scan tasks that come with Command AntiVirus and the scan tasks that you create are **System Tasks**. These **System Tasks** can be created by both users and administrators.



In Windows NT, Windows 2000, and Windows XP, two types of scans can be created:

- **System Tasks** – Scans created by someone who is signed on as a member of the Administrators group on the local machine. You can identify a **System Task** by the computer icon  located to the left of the scan task name.
- **User Tasks** – Scans created by a user who is **not** signed on as a member of the Administrators group on the local machine. You can identify a **User Task** by the profile icon  located to the left of the scan task name.

The preset scan tasks that come with Command AntiVirus are **System Tasks**.



NOTE: A user who is signed on as a member of the Administrators group on the local machine can create either type of task.



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

Changing Task Names



In Windows NT, Windows 2000, and Windows XP, if you are **not** signed on as a member of the Administrators group on the local machine, you can change the name of **User Tasks**, but **not** the name of **System Tasks**.

To rename a scan task, follow these steps:

1. Select the scan task, and click once. The system displays a text box around the existing name.



NOTE: Using the right mouse button (right-click), you can also click the scan task and select **Rename** from the drop-down menu.

2. Type the new name, and 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.

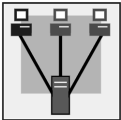
If you make an error while you are typing, press the **Esc** key to go back to the original name.

Sorting the Order of Scan Tasks

You can sort scan tasks in the **Task List** by clicking the column headers. For example, clicking the **Next scan on** header sorts scan tasks based on the next scheduled scans.

Updating the Task Window Information

The **View** menu allows you to update the information in the **Task Window** to reflect the Command AntiVirus scan task information that is stored on the disk. For example, the **Task List** is updated with any new scan task that was created since opening the Command AntiVirus GUI. The **Task List** is also updated when the path to the **System** scan task folder is changed.



Updating the **Task Window** is useful when copying task files from the network.

To update the information in the **Task Window**, follow these steps:

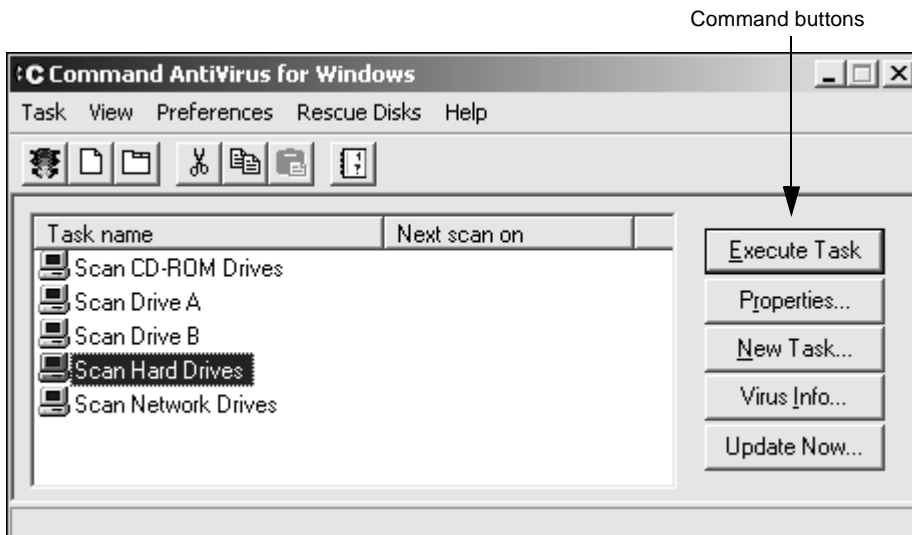
1. On the menu bar, click **View**. The system displays the **View** menu.
2. Click **Refresh**.

Sizing the Columns

You can resize the column headers by using your mouse pointer to drag the header's left or right split bar.

COMMAND BUTTONS

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



Command AntiVirus Main Dialog Box

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 **Starting an On-demand Scan** located later in this chapter.

Properties Button

This button allows you to set the properties of a scan task. Select the scan task that you want to modify, and click **Properties**. For more information on setting up a scan task, refer to **Setting Scan Task 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 A New Scan Task** 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**.

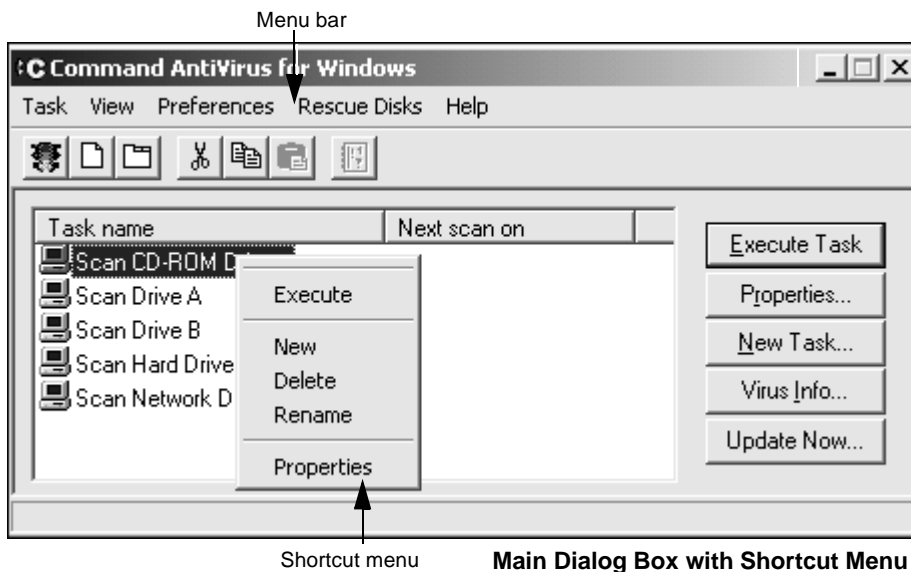
Update Now Button

This button allows the end-user to update the Command AntiVirus virus definition files, components, and full product on-demand. For more information, refer to **Updating Command AntiVirus** located later in this chapter.

SHORTCUT MENU

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

You can quickly access the shortcut menu by selecting a scan task and clicking the right mouse button (right-clicking).



Main Dialog Box with Shortcut Menu

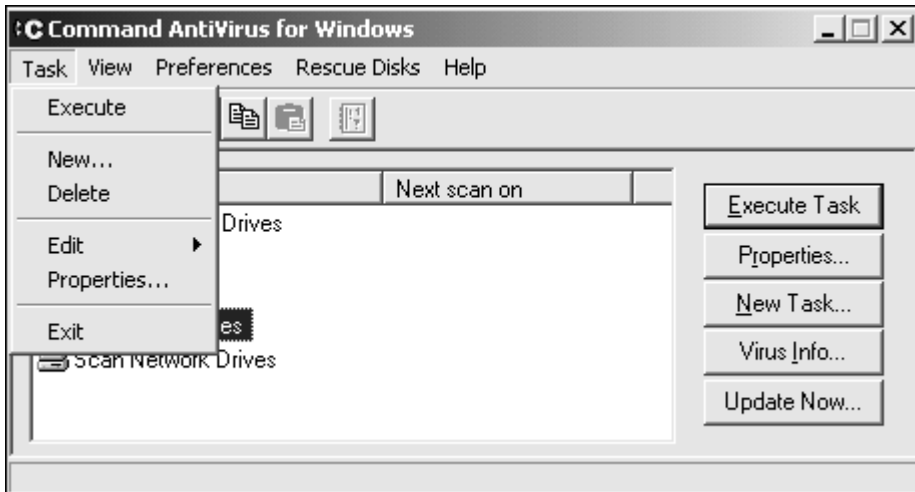
MENU BAR

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. You can also use the keyboard by pressing the **ALT** key plus the first letter of 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 view scan results, customize Command AntiVirus, create a recovery Rescue Disk set, or view topics that contain helpful information.

Task Menu

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



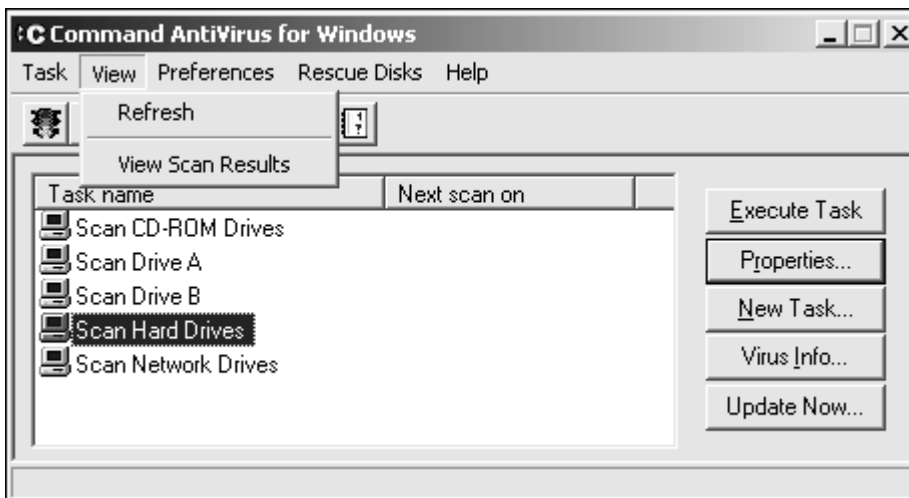
Main Dialog Box with Task Menu

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

- **Execute** – Start an on-demand scan task. For more information, refer to **Starting an On-demand Scan** located later in this chapter.
- **New** – Create a new scan task. For more information, refer to **Creating a New Scan Task** located later in this chapter.
- **Delete** – Remove a scan task. For more information, refer to **Deleting a Scan Task** located later in this chapter.
- **Edit** – Copy an existing scan task. For more information, refer to **Copying a Scan Task** located later in this chapter.
- **Properties** – Modify the features of a scan task. For more information, refer to **Setting Scan Task Properties** located later in this chapter.
- **Exit** – Close the **Command AntiVirus Main** dialog box.

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 update the information in the **Task Window** and to view scan results.

For more information on updating the Task Window, refer to **Updating the Task Window Information** located previously in this chapter.

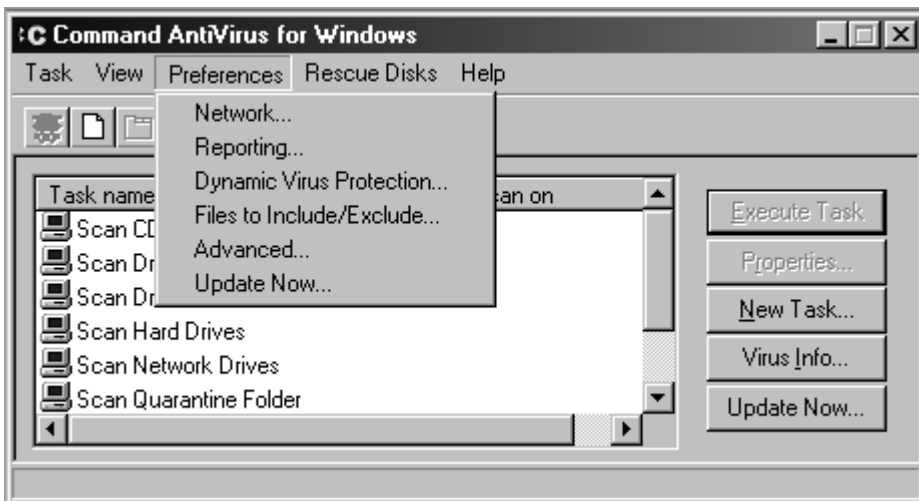
For more information on viewing scan results, refer to **Viewing Scan Results** located later in this chapter.

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.



In Windows NT, Windows 2000, and Windows XP, to change **Preferences**, you **must** be signed on as a member of the Administrators group on the local machine. If you are not, all of the menu items except **Advanced** are available **only** for viewing.



Main Dialog Box with Preferences Menu

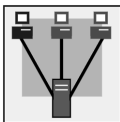
The items on the **Preferences** menu allow you to:

- **Network** – Specify how CSAV behaves when scanning a network drive that has NetWare installed. For more information, refer to **Setting CSAV Scanning Options for NetWare Drives** located later in this chapter.



NOTE: The **Network** menu item is available **only** if you have the Novell® NetWare® client installed.

- **Reporting** – Control how and where scan results are reported, modify the message CSAV displays when a virus infection is found during a manual, and set an audible virus warning. For more information, refer to **Customizing Scan Results Reporting** located later in this chapter.



Administrators can also set CSAV to mail a virus report to a recipient and/or to log virus infections found to a NetWare server. For more information, refer to **Sending a Virus Notification Message** and/or **Setting Up Virus Reporting to a NetWare Server** located later in this chapter.

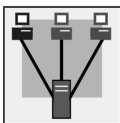
- **Dynamic Virus Protection** – Start, or stop on-access scanning protection. You can also set the on-access scanning properties including the action that Command AntiVirus takes when it detects a virus infection through on-access scanning. For more information, refer to **Setting On-access Scanning Properties** located later in this chapter.
- **Files to Include/Exclude** – Specify additional file types to **Include** in and what files and/or directories to **Exclude** from all scans. For more information, refer to **Specifying Files/Directories To Scan** located later in this chapter.
- **Advanced** – Set the path of the quarantine folder, receive a warning if the virus definition files are out-of-date, and change the folder containing the Command AntiVirus **System Task** files.



In Windows NT, Windows 2000, and Windows XP, the **Advanced** menu item is available **only** if you are signed on as a member of the Administrators group on the local machine.

For more information on changing the quarantine folder, refer to **Using the Quarantine Feature** located later in this chapter.

For more information on how to receive a warning if the virus definition files are out-of-date, refer to **Setting a Virus Definition Files Warning** located later in this chapter.



For more information on changing the Command AntiVirus **System Task** files folder, refer to **Changing the System Scan Task Folder** located later in this chapter.

- **Update Now** – Check for definition file updates, component updates, and/or product upgrades automatically, select the site from which you download the updated files, and select whether or not you want to be notified when updated files are available. For more information, refer to **Updating Command AntiVirus** located later in this chapter.

Rescue Disks Menu

You can access the **Rescue Disks** menu by clicking **Rescue Disks** on the menu bar:



Main Dialog Box with Rescue Disks Menu

The **Rescue Disks** menu allows you to create a recovery Rescue Disk set. For more information, refer to **Creating and Using a Rescue Disk Set** located later in this chapter.

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:



Main Dialog Box with Help Menu

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

- **Help** – Find information on a specific topic
- **Readme.txt** – View the Readme.txt file
- **Technical Support** – Contact your local Technical Support representative
- **Virus Information** – View a list of viruses handled by Command AntiVirus
- **About** – View the Command AntiVirus product installation information

For more information, refer to **Getting Help** located 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 view scan results. Just click the appropriate button.

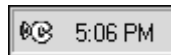


NOTE: To see a ToolTip that identifies the function of a particular button, move the mouse pointer over any toolbar button.

OTHER WAYS TO ACCESS COMMAND ANTIVIRUS

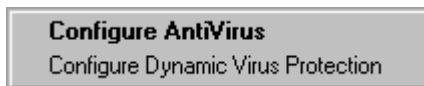
You can open the **Command AntiVirus Main** dialog box in several ways:

- From the **Start** menu.
- By double-clicking the yellow **C** icon (Command AntiVirus notification icon) in the Windows notification area located to the right of the Windows Quick Launch bar:



CSAV Icon

- By right-clicking the yellow **C** icon in the Windows notification area, and then clicking **Configure AntiVirus** from the **Command AntiVirus Shortcut Menu**:



Command AntiVirus Shortcut Menu

The **Command AntiVirus** shortcut menu also allows you to set the properties of on-access scanning protection provided through Dynamic Virus Protection (DVP). Just click the **Configure Dynamic Virus Protection** menu item. The system displays the **Dynamic Virus Protection** dialog box. For more information on setting the scanning properties of DVP, refer to **Setting On-access Scanning Properties** located later in this chapter.

CREATING AND USING A RESCUE DISK SET

Some viruses may prevent you from starting up your system or accessing your Command AntiVirus program. A **Rescue Disk** set helps you to detect and remove these viruses.

The **Rescue Disks** menu in the Command AntiVirus graphical user interface (GUI) allows you to create a **Rescue Disk** set. You can access this menu by clicking **Rescue Disks** 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.

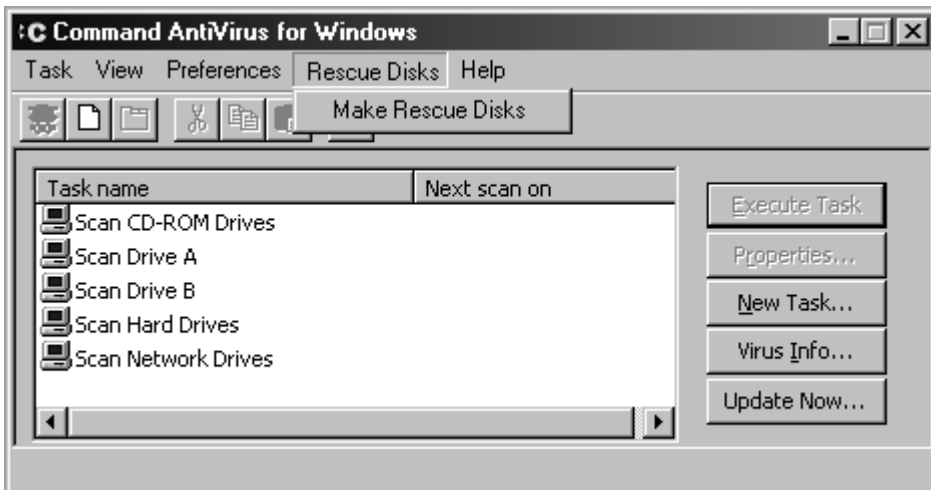
You can use **Rescue Disk 1** on NTFS systems at any time to repair damaged or infected boot sector information.

This section contains information on how to create a **Rescue Disk** set from the Command AntiVirus **Rescue Disks** menu and how to use the **Rescue Disk** set when you cannot use your Command AntiVirus program.

CREATING FROM THE RESCUE DISKS MENU

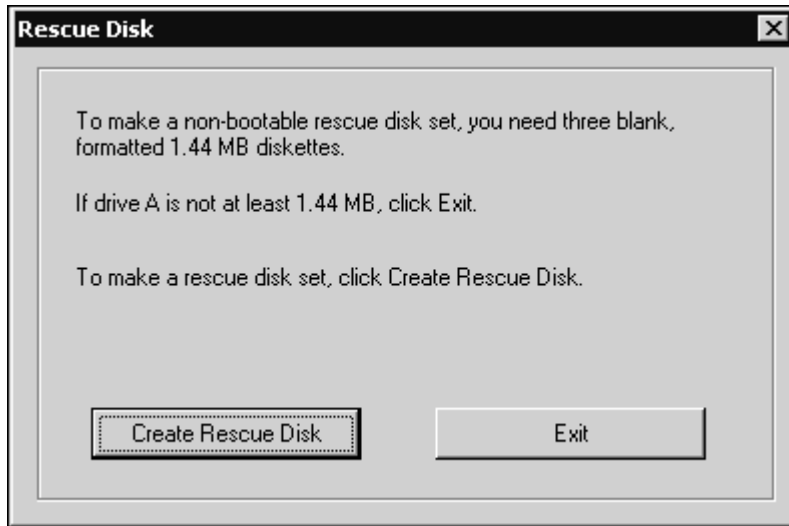
To create a **Rescue Disk** set from the **Rescue Disks** menu, follow these steps:

1. On the Command AntiVirus menu bar, click **Rescue Disks**. The system displays the **Rescue Disks** menu:



Rescue Disks Menu

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

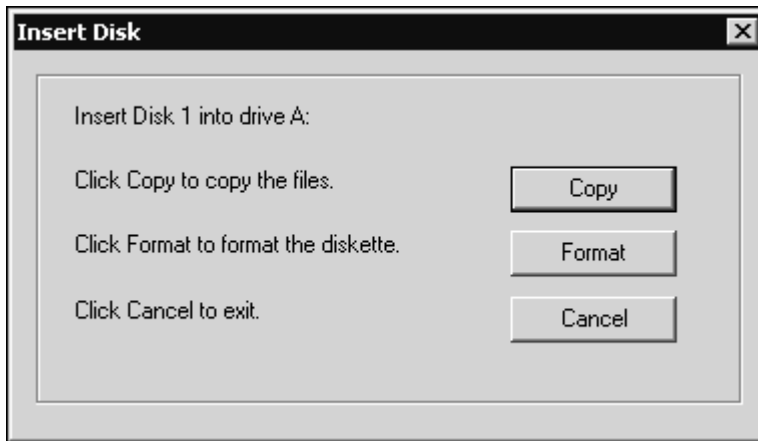


Rescue Disk Dialog Box



NOTE: If drive A is not at least 1.44MB, 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 Dialog Box

4. Insert **Disk 1** into drive A, and click **Copy**. The system displays the **Copying** dialog box that shows the files being copied.

When the copying is complete, the system returns to the **Insert Disk** dialog box which prompts you for **Disk 2**.



NOTE: If your disk is **not** formatted, insert **Disk 1**, and 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. 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.

6. Insert **Disk 2** into drive A, and click **Copy**. The system displays the **Copying** dialog box that shows the files being copied.

When the copying is complete, the system returns to the **Insert Disk** dialog box which prompts you for **Disk 3**.

7. Remove **Disk 2** from drive A, and set the write-protect tab to prevent any modifications.
8. Insert **Disk 3** into drive A, and click **Copy**. The system displays the **Copying** dialog box that shows the files being copied.

When the copying is complete, the system returns to the **Command AntiVirus Main** dialog box.

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

If necessary, you can run a Command AntiVirus scan from the **Rescue Disk** set.

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



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

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

USING THE RESCUE DISK SET

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

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

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

6. At the A prompt, type the following:

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

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

When the scan is complete, remove **Rescue Disk 3** from drive A.

STARTING AN ON-DEMAND SCAN

Periodically performing an on-demand scan of your diskette drives, local hard drives, network drives, or CD-ROM drives is an important part of keeping your system virus free.

You can perform this task quickly and easily by using the preset scan tasks that come with Command AntiVirus. These tasks are the most commonly needed tasks, and they are set with the more common scan task properties. By default, they are set to disinfect when a virus infection is found.

You can start an on-demand scan from the **Task** menu, the Windows shortcut menu, or the command line. You can also schedule an on-demand scan task to run daily, weekly, or monthly at a particular time of the day. For more information on scheduling an on-demand scan, refer to **Scheduling An On-demand Scan** located later in this chapter.

Command AntiVirus allows you to change the features of a scan task through the **Properties** dialog box. For example, you can select a particular path or folder to scan, specify the action to take when a virus infection is found, and select the types of files to include in or exclude from a scan. For more information, refer to **Setting Scan Task Properties** located later in this chapter.

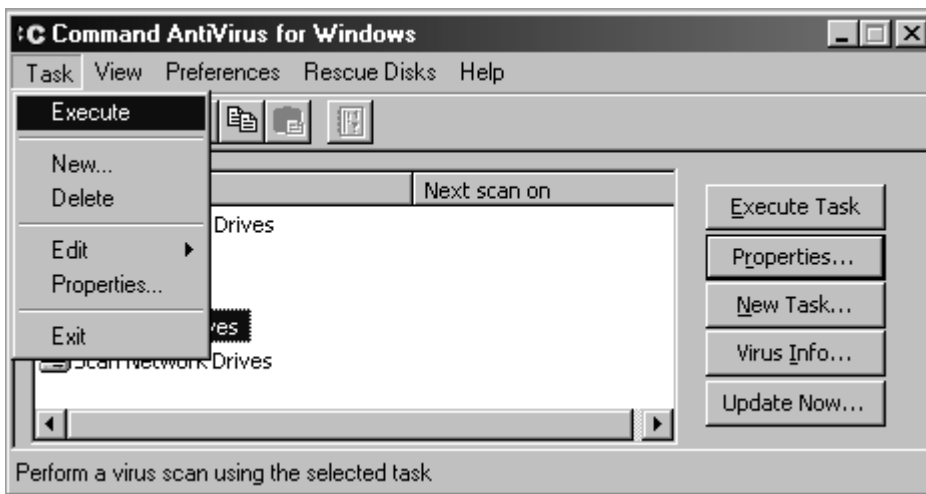
You can also create a new scan task through the **Task** menu. For more information, refer to **Creating A New Scan Task** located later in this chapter.

This section contains information on how to start an on-demand scan from the Command AntiVirus **Task** menu, from the Windows shortcut menu, and from the Windows command line.

FROM THE TASK MENU

To start an on-demand scan from the **Task** menu, follow these steps:

1. From the **Task List** in the **Command AntiVirus Main** dialog box, select a **Task name** for example, **Scan CD-ROM Drives**.
2. On the Command AntiVirus menu bar, click **Task**. The system displays the **Task** menu:

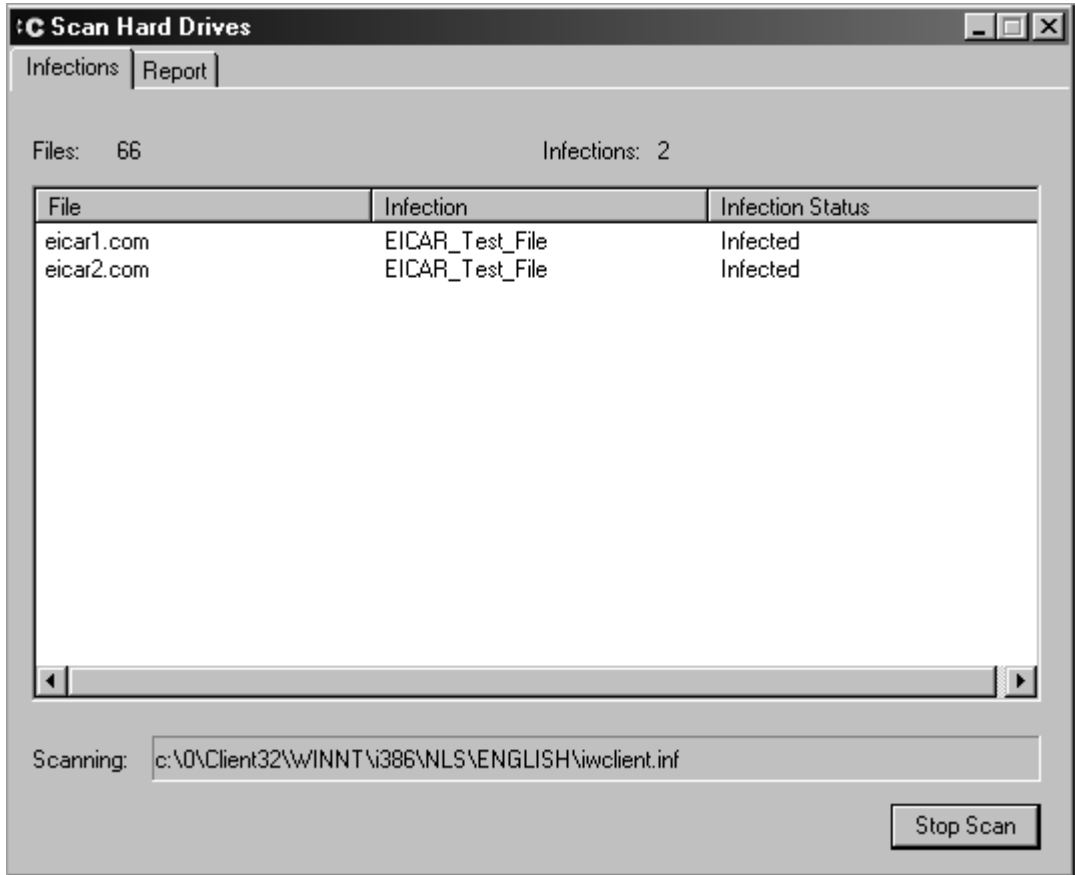


Task Menu

3. Click **Execute**. The scan begins, and the system displays the **Scan** dialog box with the **Infections** dialog box in view.



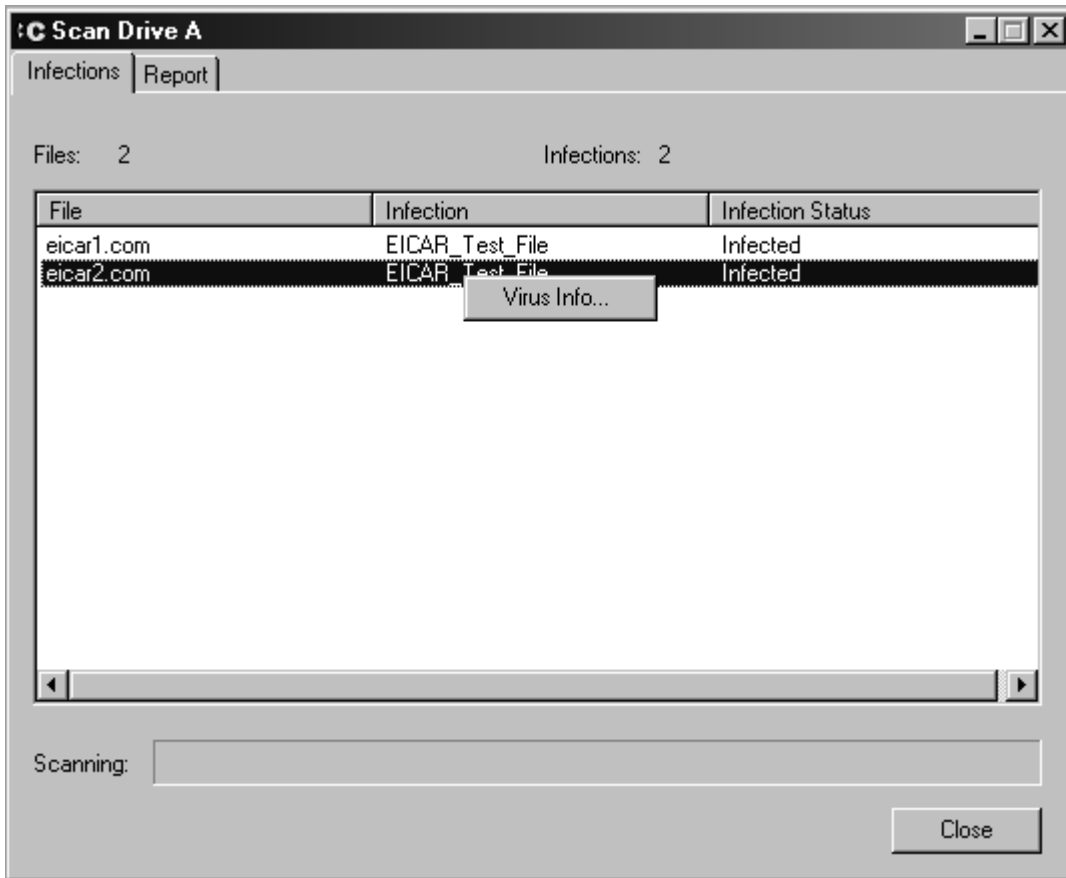
NOTE: You can stop the scan at any time by clicking the **Stop Scan** button. When the scan is complete, **Stop Scan** changes to **Close**. You can then click the **Close** button to exit the **Scan** dialog box.

**Infections Dialog Box**

This dialog box provides details about the scan that is taking place:

- **Files** – Progressively displays the number of files scanned.
- **Infections** – Progressively displays the number of virus infections found.

- **File** – Identifies the file that contains a virus infection. To display the location of the infected file, using the mouse, point to the file name.
- **Infection** – Identifies the type of virus infection found. To go to our web site to find out more information about the infection, right-click the **Infection** name. The system displays a drop-down menu:



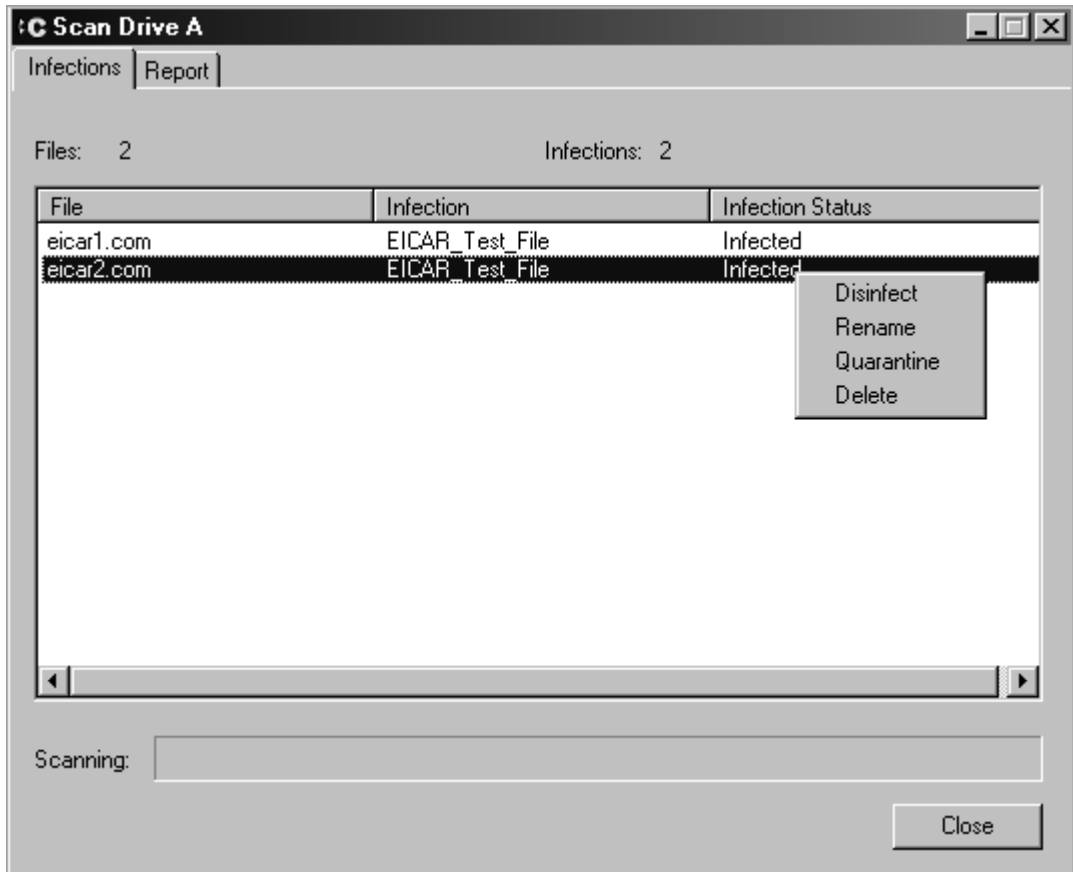
Infections Dialog Box – Virus Info

Click **Virus Info**. You are connected to the virus search page of the Command Software web site. This page provides links to additional information about the virus infection that was found and the ability to search for information on other infections.



NOTE: To obtain this information, you **must** be connected to the Internet.

- **Infection Status** – Identifies the present state of the virus infection, for example, **Infected**. To change the status, right-click the specified **Infection Status**. The system displays a drop-down menu:



Infections Dialog Box – Action On Infection

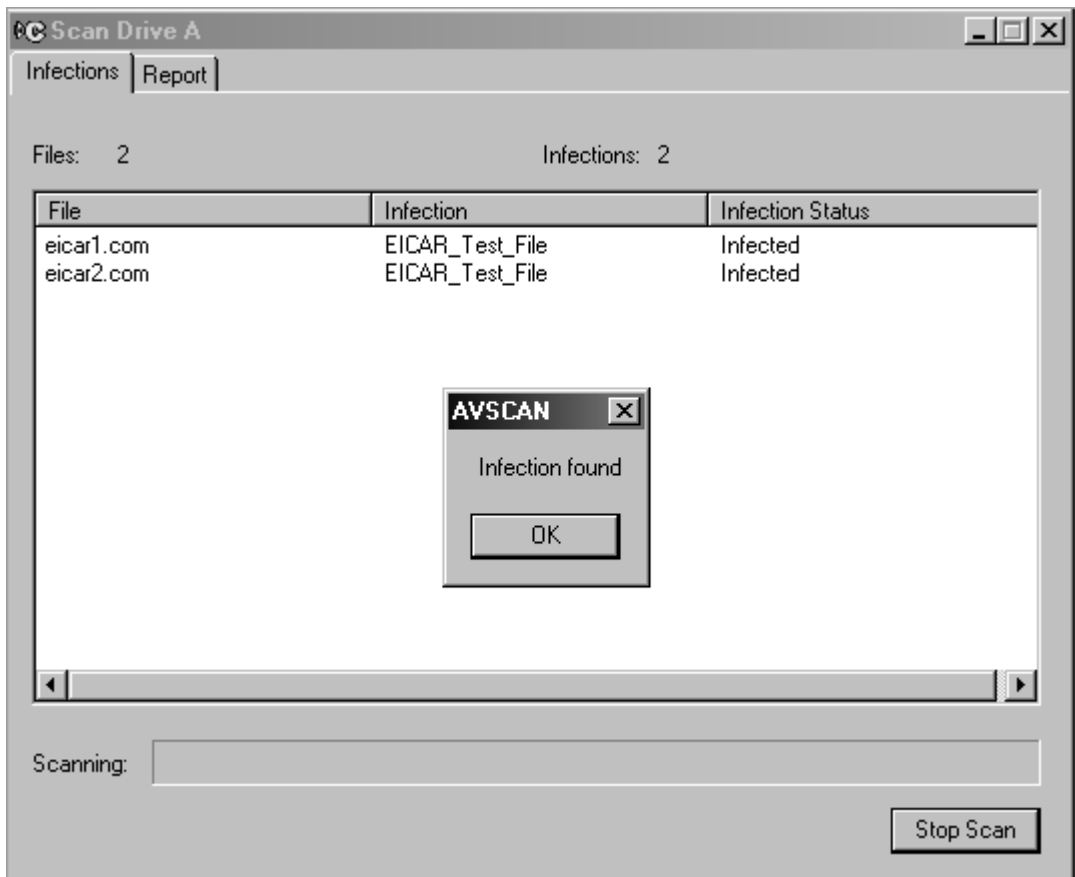
This menu allows you to **Disinfect**, **Rename**, **Quarantine**, or **Delete** the infected file. Click the action that you want to take, for example, **Disinfect**. CSAV disinfects the file and changes the **Infection Status** to **Disinfected**.



NOTE: The default setting for **Action on infection** in Command AntiVirus is **Disinfect**. You can change the default setting for both on-demand and on-access scanning. For more information refer to **Setting Scan Task Properties** and **Setting On-access Scanning Properties** located later in this chapter.

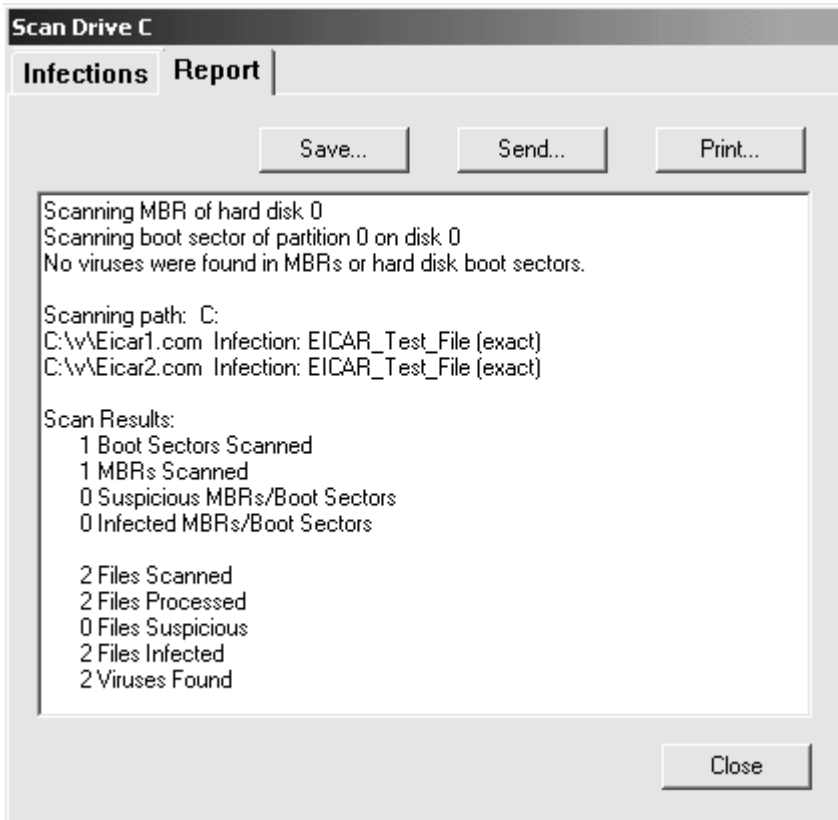
- **Scanning** – Identifies the file currently being scanned.

When the scan is complete, the system displays an **AVSCAN** message box, for example:



AVScan Message Box

4. Click **OK** to close the message box.
5. Click the **Report** tab. The system displays the **Report** dialog box:




Report Dialog Box

This dialog box provides a summary of the scan details. It also allows you to save a copy of the report, send a copy of the report through your e-mail system, or print the report by clicking the **Save**, **Send** or **Print** buttons.

6. Click **Close** to close the **Scan** dialog box.



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.

FROM THE WINDOWS SHORTCUT MENU

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

To perform a scan from the Windows 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 menu containing the **Command AntiVirus Scan** option:



Shortcut Menu Scan

3. Click **Command AntiVirus Scan**. The scan begins immediately, and the system displays the **AVScan** dialog box with the **Infections** dialog box in view.



NOTE: The shortcut or right-click scanning properties are based on the Command AntiVirus default scanning properties. For example, if a virus infection is found, CSAV attempts to disinfect the file. For more information, refer to **Setting Scan Task Properties** located later in this chapter.

You can also take action on a particular virus from the **Infections** dialog box when you are running a scan.

FROM THE COMMAND LINE

Command AntiVirus includes a program called **CSAV.EXE** that you can use to run a scan from the command line.

CSAV.EXE is an operating system-specific command-line scanner. 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\Command AntiVirus** folder.

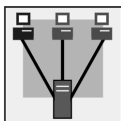
SCHEDULING AN ON-DEMAND SCAN

To help you keep your system virus free, you can schedule an on-demand scan task to run daily, weekly, or monthly at a particular time of the day. Scheduling a daily scan guarantees that your computer is consistently checked for virus infections. You can schedule an on-demand scan task through the **Task/Properties/Schedule** dialog box.



In Windows NT, Windows 2000, and Windows XP, the **Schedule** dialog box is available **only** for a **System Task**.

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.



Administrators can create scheduled scans that are installed on each user's computer. These administrator-defined scheduled scans also 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 Windows notification area. If the computer is **not** on when a scan is scheduled to run, the scan is skipped.

To stop a scheduled scan once it has started, right-click the yellow **C** icon in the Windows notification area, select **Stop Scheduled scans** from the shortcut menu, and then click the scan that you want to stop, for example, **Scan Hard Drives**.

You can view the results of a scheduled scan through the **View** menu.



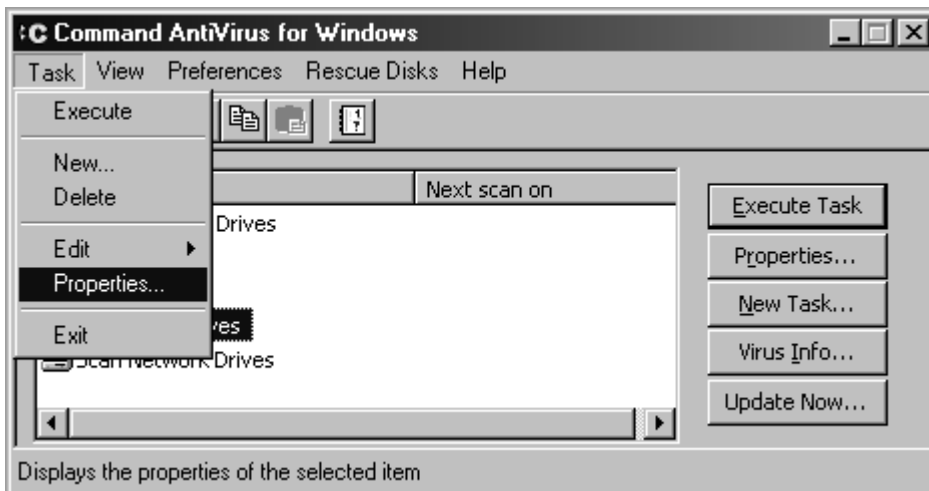
In Windows NT, Windows 2000, or Windows XP, you can also view scan results in the Windows Event Viewer if you selected the **Report to Application Log** option.

For more information, refer to **Viewing Scan Results** located later in this chapter.

This section contains information on how to schedule an on-demand scan.

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


1. In the **Command AntiVirus Main** dialog box, select a **Task name**.
2. On the menu bar, click **Task**. The system displays the **Task** menu:



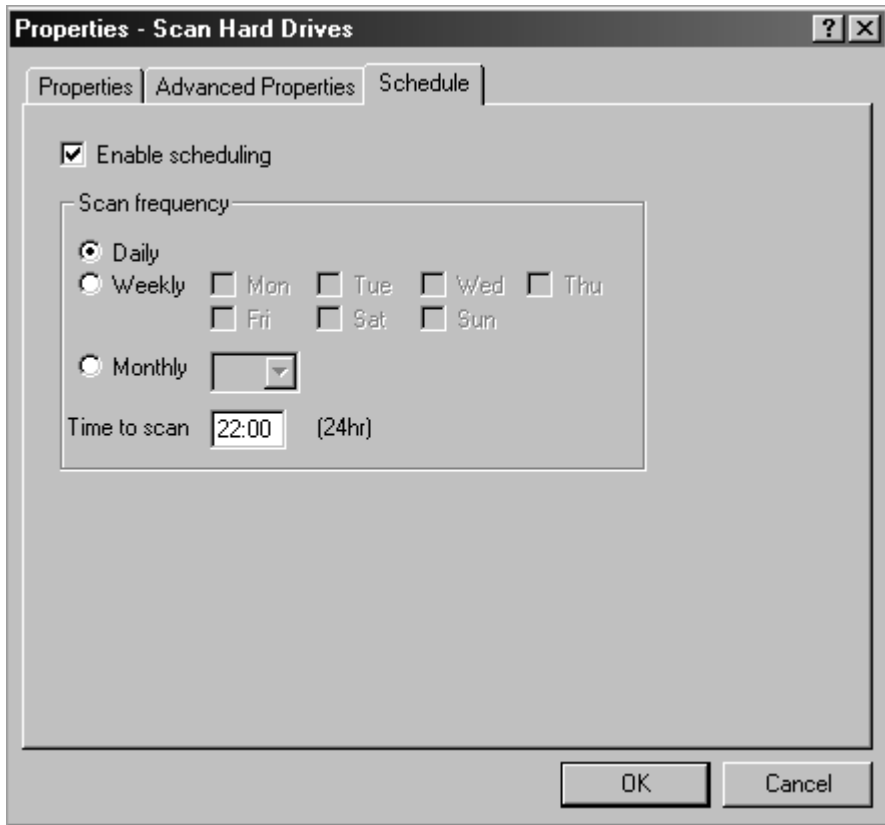
Task Menu

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 the **Schedule** tab. The system displays the **Schedule** dialog box:



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 do **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. In the **Time to scan** text box, type the time of day that you want the scan to start. Use a 24-hour format with “00.00” indicating midnight. 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 want to schedule an immediate scheduled scan for testing purposes, you should schedule the scan at least one minute ahead of the current time. For example, if the current time is 10:44 a.m., set the **Time to scan** to 10:45.

8. Click OK.

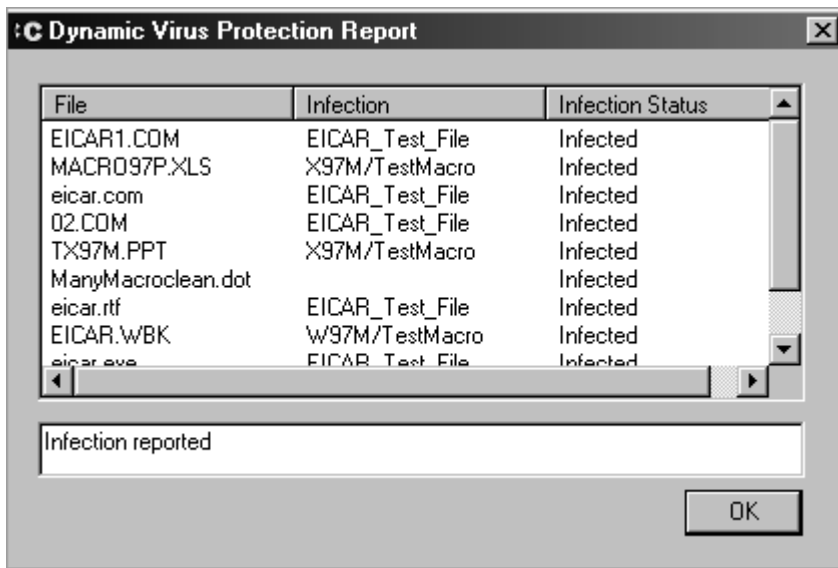
UNDERSTANDING ON-ACCESS SCAN REPORTING

On-access scanning protection through Dynamic Virus Protection (DVP) works “behind the scenes” to protect your system from becoming infected by a computer virus. When DVP finds a virus-infected file, the system displays the **Dynamic Virus Protection Report** log.



NOTE: The **DVP Report** log may open in the background. Just click **Dynamic Virus Protection** in the Windows Quick Launch bar to bring the log forward.

This section contains a description of the information that is contained in the **DVP Report** log. It also provides information on how to view the information in the log, clear the log, and exit the log.



DVP Report Log

The **Dynamic Virus Protection Report** log provides the following information for **all** virus infections found during a login session.



NOTE: As the **Dynamic Virus Protection Report** log can be cleared, the log may not contain the scan results of previous DVP scanning during that session.

- **File** – Identifies the file that contains a virus infection. To display the location of the infected file, using the mouse, point to the file name.
- **Infection** – Identifies the type of virus infection found.
- **Infection Status** – Identifies the present state of the virus infection, for example, **Infected**.



NOTE: To view all of the infections in the log, or to view all of the information on each infection, use the scroll bars. To exit, click the **OK** button.

Clearing the Scan Results

To clear the entire log, right-click a **File**, and then click **Clear All**.

To clear a single item from the log, right-click the **File**, and then click **Clear Selection**.

VIEWING SCAN RESULTS

You can view the results of on-demand scans including scheduled scans and the results of on-access scanning through DVP from the **View** menu.



In Windows NT, Windows 2000, or Windows XP, you can also view scan results in the Windows Event Viewer if you selected the **Report to Application Log** option.

This section contains information on how to view scan results from both the **View** menu and the Windows Event Viewer. It also contains information on how to log results to the Windows Event Viewer Application Log.

FROM THE VIEW MENU

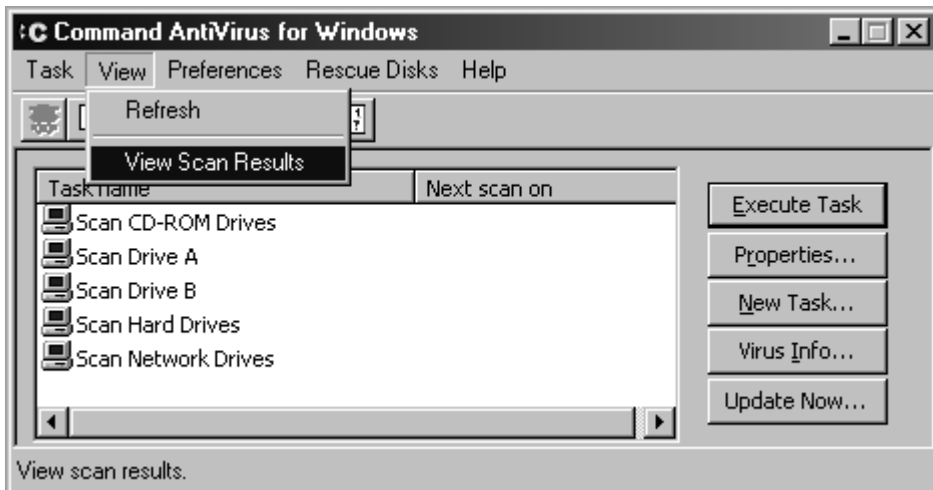
The **View** menu allows you to view the scan results of **all** on-demand scans including scheduled scans and the scan results of DVP scanning. You can view this list of scan results in the **View/View Scan Results/Command AntiVirus Scan Results** dialog box.



You can also view the **Command AntiVirus Scan Results** by clicking the **View Scan Results** button on the toolbar.

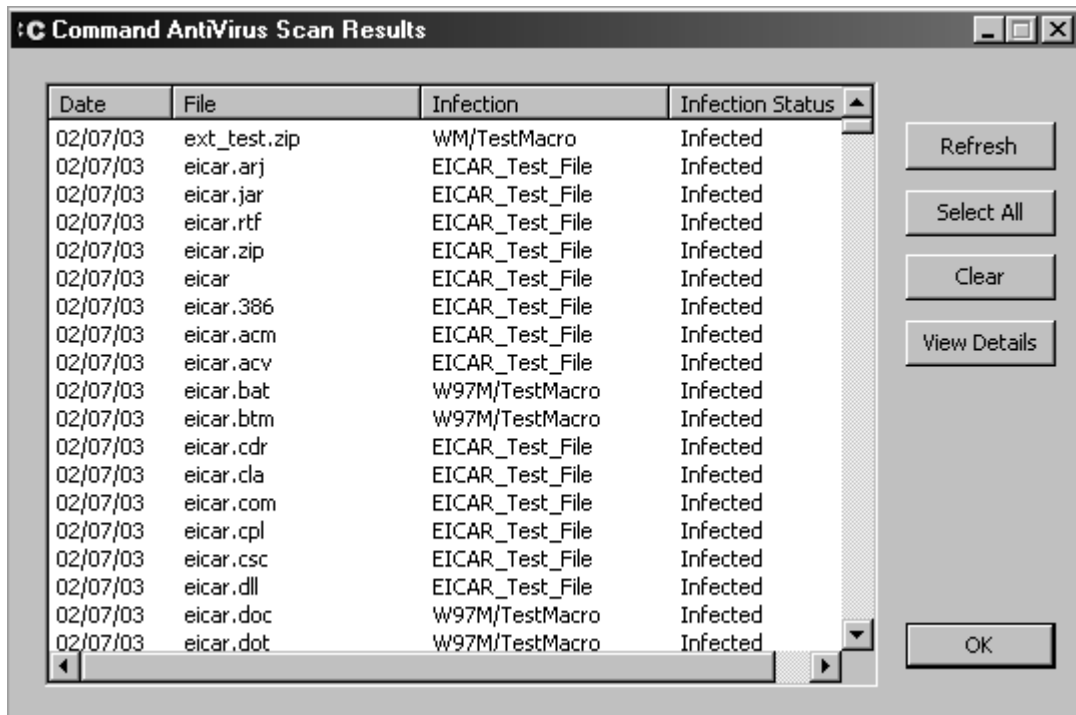
To view scan results from the **View** menu, follow these steps:

1. On the Command AntiVirus menu bar, click **View**. The system displays the **View** menu:



View Menu

2. Click **View Scan Results**. The system displays the **Command AntiVirus Scan Results** log:



The screenshot shows a window titled "Command AntiVirus Scan Results". It contains a table with four columns: Date, File, Infection, and Infection Status. The table lists 18 files, all dated 02/07/03, with various infection types and a status of "Infected". To the right of the table are buttons for "Refresh", "Select All", "Clear", "View Details", and "OK".

Date	File	Infection	Infection Status
02/07/03	ext_test.zip	WM/TestMacro	Infected
02/07/03	eicar.arj	EICAR_Test_File	Infected
02/07/03	eicar.jar	EICAR_Test_File	Infected
02/07/03	eicar.rtf	EICAR_Test_File	Infected
02/07/03	eicar.zip	EICAR_Test_File	Infected
02/07/03	eicar	EICAR_Test_File	Infected
02/07/03	eicar.386	EICAR_Test_File	Infected
02/07/03	eicar.acm	EICAR_Test_File	Infected
02/07/03	eicar.acv	EICAR_Test_File	Infected
02/07/03	eicar.bat	W97M/TestMacro	Infected
02/07/03	eicar.btm	W97M/TestMacro	Infected
02/07/03	eicar.cdr	EICAR_Test_File	Infected
02/07/03	eicar.cla	EICAR_Test_File	Infected
02/07/03	eicar.com	EICAR_Test_File	Infected
02/07/03	eicar.cpl	EICAR_Test_File	Infected
02/07/03	eicar.csc	EICAR_Test_File	Infected
02/07/03	eicar.dll	EICAR_Test_File	Infected
02/07/03	eicar.doc	W97M/TestMacro	Infected
02/07/03	eicar.dot	W97M/TestMacro	Infected

CSAV Scan Results Log

The **Command AntiVirus Scan Results** log provides the following information for **all** virus infections found.



NOTE: As the **Command AntiVirus Scan Results** log can be cleared, the log may not contain the scan results of previous scans.

- **Date** – Specifies the date the virus infection was found.
- **File** – Identifies the file that contains a virus infection. To display the location of the infected file, right-click the **File**, and click **Details**.

- **Infection** – Identifies the type of virus infection found.
- **Infection Status** – Identifies the present state of the virus infection, for example, **Infected**.

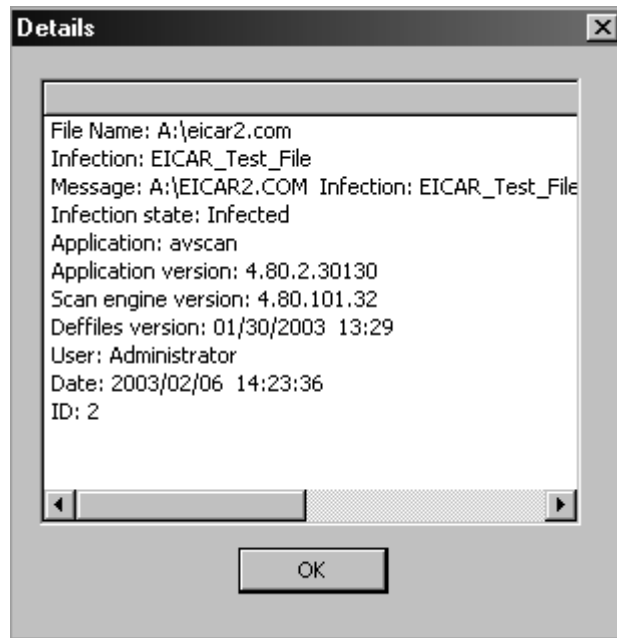


NOTE: To view all of the infections in the list, or to view all of the information on each infection, use the scroll bars. To exit, click the **OK** button.

Viewing Scan Results Details

To view the details of a single file in the log, right-click the **File**, and click **Details**.

To view the details of all of the files in the log, click the **Select All** button, and then click the **View Details** button.



Details Dialog Box

Adding the Latest Scan Results

To add the latest scan information to the list, click the **Refresh** button.

Clearing the Scan Results

To clear the entire log, click the **Select All** button, and then click the **Clear** button.

To clear a single item from the log, right-click the **File**, and then click **Clear Selection**.

Receiving an Infection Warning

If your computer contains a virus infection that has been detected through DVP scanning or an on-demand scan including a scheduled scan, Command AntiVirus displays the following **Command AntiVirus Infection Warning** dialog box when you log on to your computer:



CSAV Infection Warning Dialog Box

This dialog box allows you to view the **Command AntiVirus Scan Results** log to determine what type of infection has been found. Command AntiVirus continues to display this dialog box at login until you take some action on the infected file, for example, **Disinfect**.

IN THE WINDOWS EVENT VIEWER



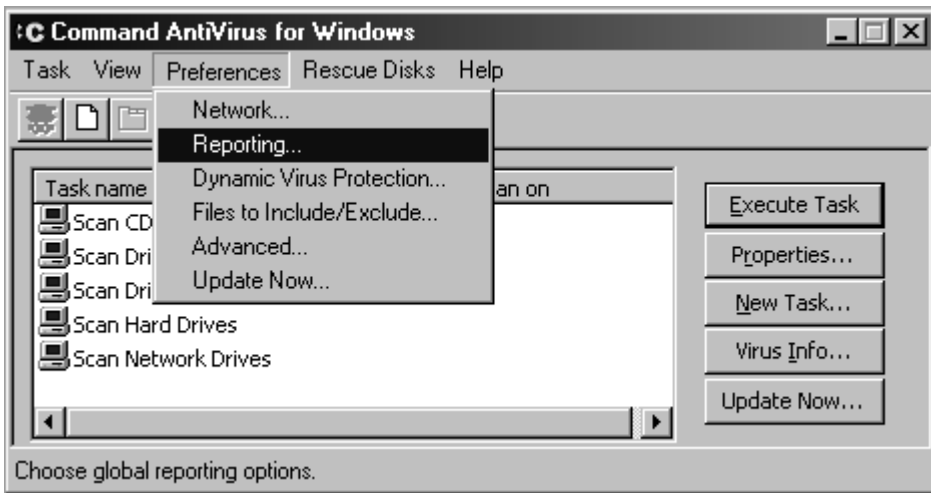
This information is **only** for Windows NT, Windows 2000, or Windows XP.

You can log each occurrence of a virus found during an on-demand scan including a scheduled scan and in real time through DVP to the operating system's **Event Viewer Application Log**.

Logging Scan Results

To log each occurrence of a virus found in the **Event Viewer Application Log**, follow these steps:

1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Preferences Menu

2. Click **Reporting**. The system displays the **Reporting** dialog box with the **General** dialog box in view:



General Dialog Box

3. Select the **Report to Application Log** check box.
4. Click **OK**.

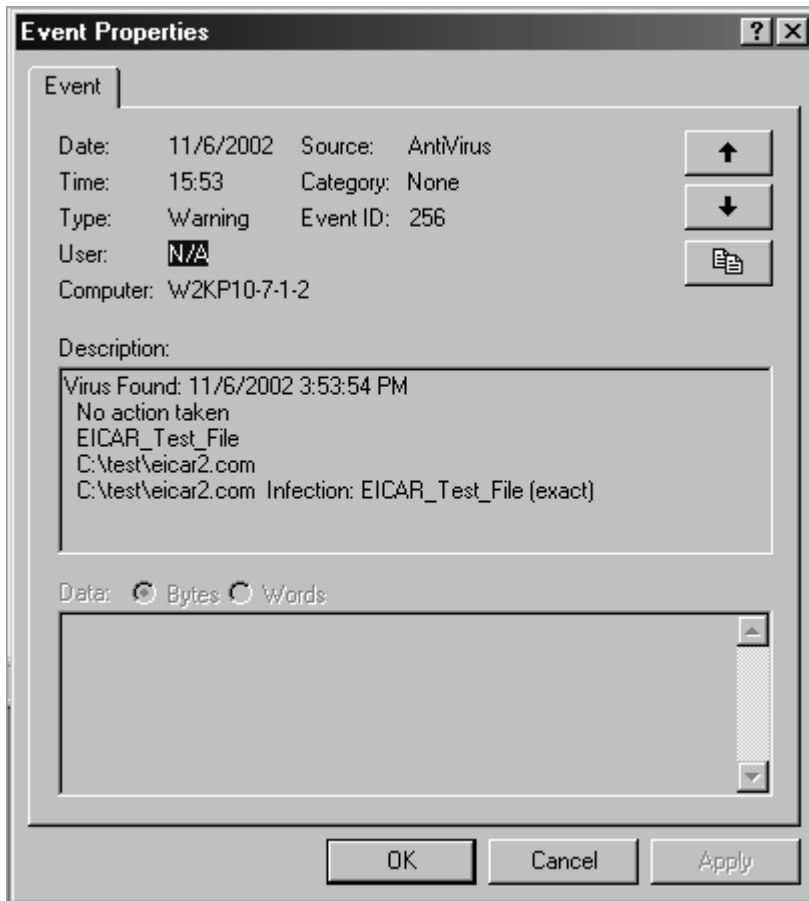


The Event Viewer log may become filled if Command AntiVirus finds a large number of infected files. If that happens frequently, you might consider increasing the **Maximum Log Size** in Event Viewer. Consult your operating system's manual for further information.

Locating Scan Results

To locate an event, follow these steps:

1. Open **Event Viewer**.
2. Select **one** of the following:
 - **In Windows 2000 and Windows XP** – select **Application Log**.
 - **In Windows NT** – On the menu bar, click **Log**, and select **Application**.
3. In the **Source** column of the log look for **AntiVirus**.
4. Double-click the event to view the **Event Properties** or **Event Detail** dialog box:



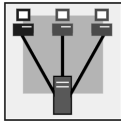
Event Properties Dialog Box

The **Event Properties** dialog box provides specific information on the virus infections that were found during the scan.

CUSTOMIZING SCAN RESULTS REPORTING

Through the **Preferences/Reporting** dialog box you can control how and where scan results are reported, modify the message Command AntiVirus displays when a virus infection is found during a manual, and set an audible virus infection warning.

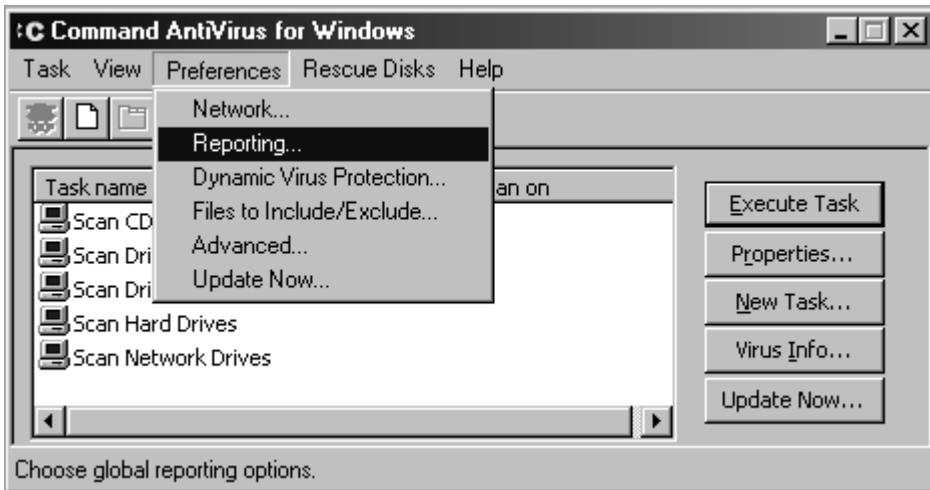
This section contains information on how to set these scan reporting options.



Administrators can also set CSAV to mail a virus infection report to a recipient and/or to log virus infections found to a NetWare server. For more information, refer to **Sending a Virus Notification Message** and/or **Setting Up Virus Reporting To a NetWare Server** located later in this chapter.

To set the reporting options, follow these steps:

1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Preferences Menu

2. Click **Reporting**. The system displays the **Reporting** dialog box with the **General** dialog box in view:



General Dialog Box

3. Select any of the following options:

- **Beep when an infection is found** – The PC speaker emits a short beep when a virus infection is detected.

For manual scans, the beep occurs only once after the scan is completed. For Dynamic Virus Protection (DVP) scanning, the beep occurs each time a virus infection is found.



NOTE: The **Beep** option does **not** apply to scheduled scans.

- **List all files scanned** – This option allows you to view a list of all files being scanned during a manual scan in the **Scan/Report** dialog box.

For all scheduled scans, you can view the list of scanned files if you selected to e-mail a virus report to a recipient and/or to log a virus report to a NetWare server. For more information, refer to **Sending a Virus Notification Message** and/or **Setting Up Virus Reporting to a NetWare Server** located later in this chapter.

Although this option allows you to verify that the appropriate files are being scanned, you can avoid lengthy reports by clearing this option.



NOTE: The **List all files scanned** option does **not** apply to DVP scanning.

- **Report to Application Log** – Logs each occurrence of a virus infection found during an on-demand scan including a scheduled scan and in real time through DVP to the operating system's **Event Viewer Application Log**.

For more information, refer to **Viewing Scan Results** located previously in this chapter.



The **Report to Application Log** option applies only to Windows NT, Windows 2000, or Windows XP.

4. If you want to change the message that Command AntiVirus displays when a virus infection is found during a manual scan, in the **Message to display when an infection is found** text box, type the new message. You can enter a text message of up to 255 characters in length. The default message is `Infection found.`



NOTE: The **Message to display when an infection is found** option does **not** apply to DVP scanning or scheduled scans.

5. Click **OK**.

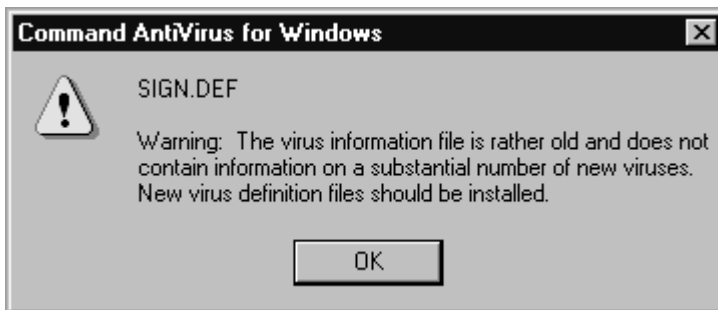
SETTING A VIRUS DEFINITION FILES WARNING



In Windows NT, Windows 2000, and Windows XP, to perform this task, you must be signed on as a member of the Administrators group on the local machine.

To ensure that your computer remains virus-free, it is important that you frequently update your Command AntiVirus virus definition files. For more information on updating, refer to **Updating Command AntiVirus** located later in this chapter.

In the **Preferences/Advanced/Miscellaneous** dialog box, you can set Command AntiVirus to provide a warning if the virus definition files are out-of-date. If you select this option, Command AntiVirus routinely checks the age of the virus definition files. When the virus definition files are older than 30 days, the system displays a warning message advising that you should update the virus definition files:

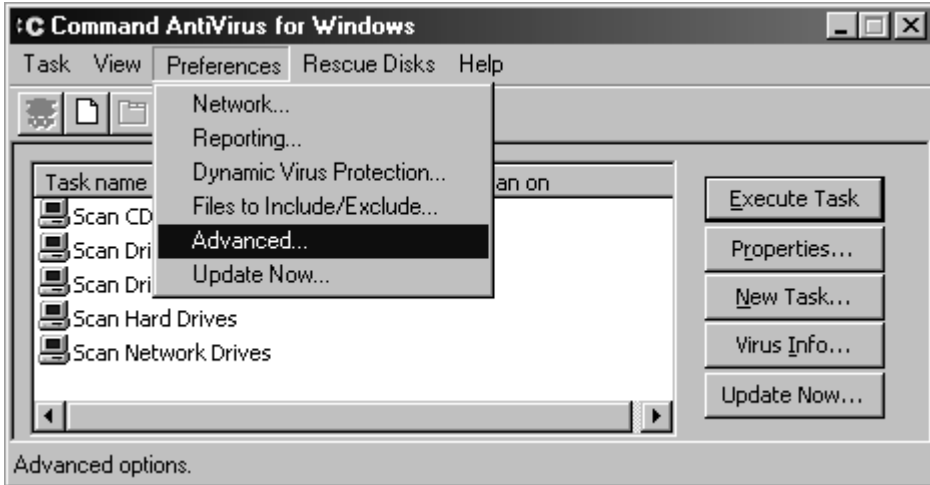


Virus Definition Files Warning Message

This section contains information on how to set Command AntiVirus to display a warning message when the virus definition files are out-of-date.

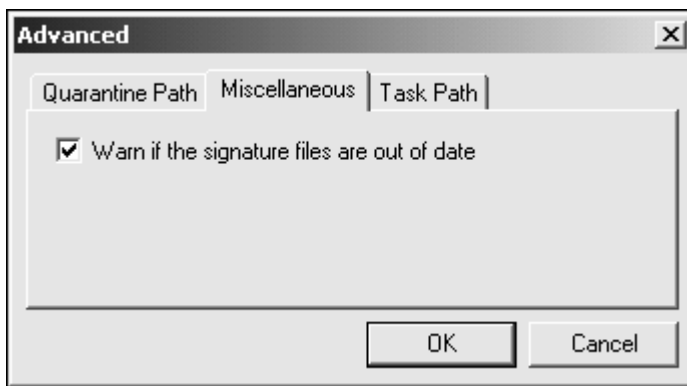
To receive a warning when the virus definition files are out-of-date, follow these steps:

1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Preferences Menu

2. Click **Advanced**. The system displays the **Advanced** dialog box.
3. Click the **Miscellaneous** tab. The system displays the **Miscellaneous** dialog box:



Miscellaneous Dialog Box

4. Select the **Warn if the signature files are out of date** check box
5. Click **OK**.

UPDATING COMMAND ANTIVIRUS

To ensure that your computer remains virus-free, it is important that you frequently update your Command AntiVirus software.

You can use the **Update Now** button in the **Command AntiVirus Main** dialog box to check for updates and upgrades of Command AntiVirus on-demand. Or, in the **Preferences/Update Now** dialog box, you can set the **Update Now** feature to check for updates automatically.

This section contains information on how to update Command AntiVirus on-demand. It also contains information on how to set Command AntiVirus to notify you when updates are available and what to do when you are notified.

CHECKING FOR UPDATES ON-DEMAND

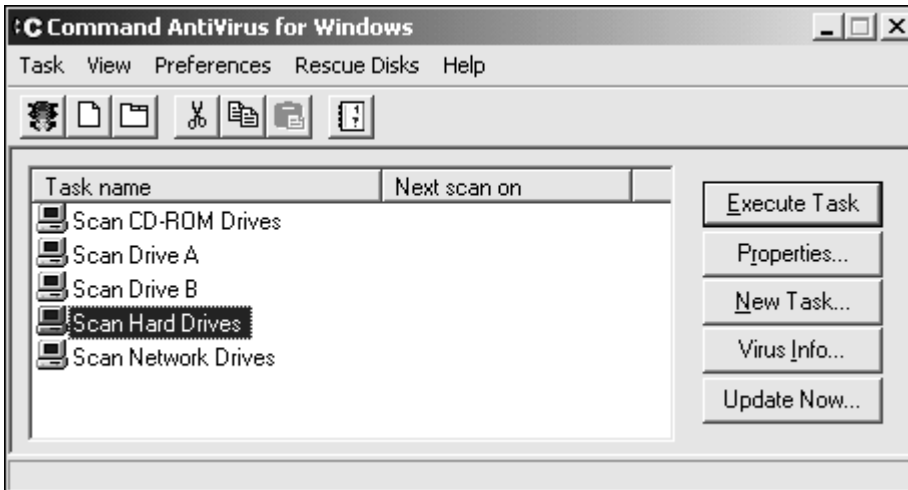


NOTE: To use the **Update Now** button, your computer **must** be connected to the Internet.



In Windows NT, Windows 2000, or Windows XP, to use the **Update Now** button, you **must** be a member of the Administrators group on the local machine.

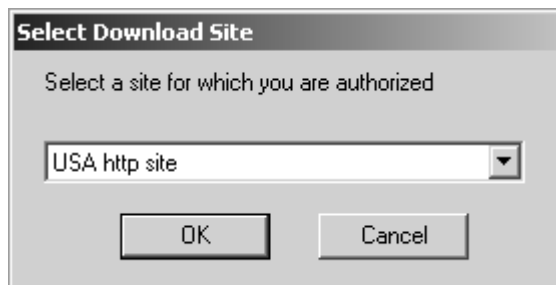
This feature allows the end-user to update the Command AntiVirus virus definition files, components, and full product on-demand by using the **Update Now** button in the **Command AntiVirus Main** dialog box:



Command AntiVirus Main Dialog Box

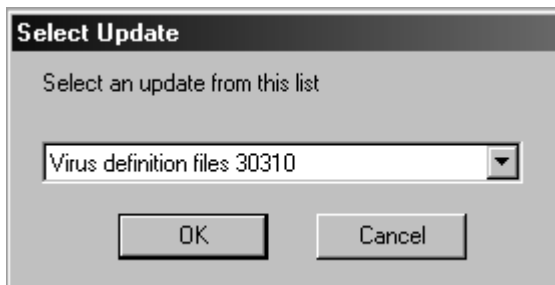
To check for updates and upgrades on-demand, follow these steps:

1. In the **Command AntiVirus Main dialog box**, click the **Update Now** button. The system displays the **Select Download Site** dialog box:



Select Download Site Dialog Box

2. From the drop-down list, select a site for which you are authorized, for example, **USA http site**.
3. Click **OK**. CSAV checks to see if there are any updates available. When the check is complete, the system displays the **Select Update** dialog box:



Select Update Dialog Box



NOTE: If there are no updates available, the system displays a dialog box informing you that there are no updates to download. Click **OK** to exit.

4. From the drop-down list, select the update or upgrade that you want to install. Available updates can include:
 - **Virus definition files** – Installs the latest virus definition files
 - **Update** – Installs the latest component update files
 - **CSAV X.XX.X** – Installs a full product upgrade of Command AntiVirus



NOTE: The x.xx.x represents the version number, for example, 4.80.0

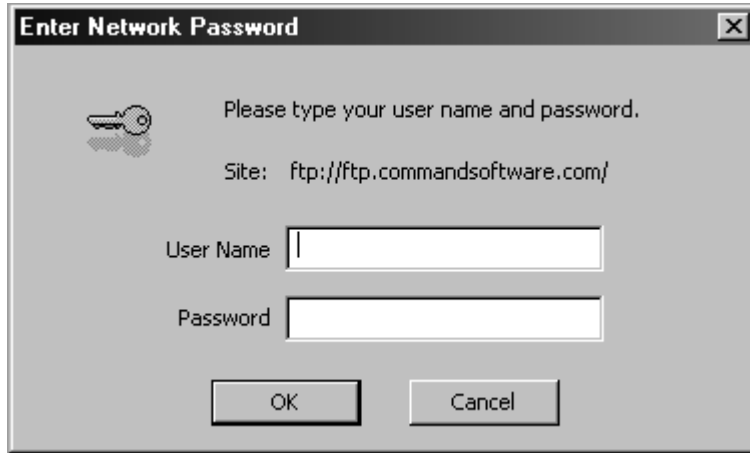
5. Click **OK**. The system displays a dialog box that asks you for your user name and password.
 - **If you selected an http site** – the system displays the following **Enter Network Password** dialog box:



Enter Network Password Dialog Box – HTTP Site

This dialog box also contains a **Save this password in your password list** check box. If you select this check box after you enter a **valid** user name and password, this dialog box does **not** display again as long as your user name and password remain valid.

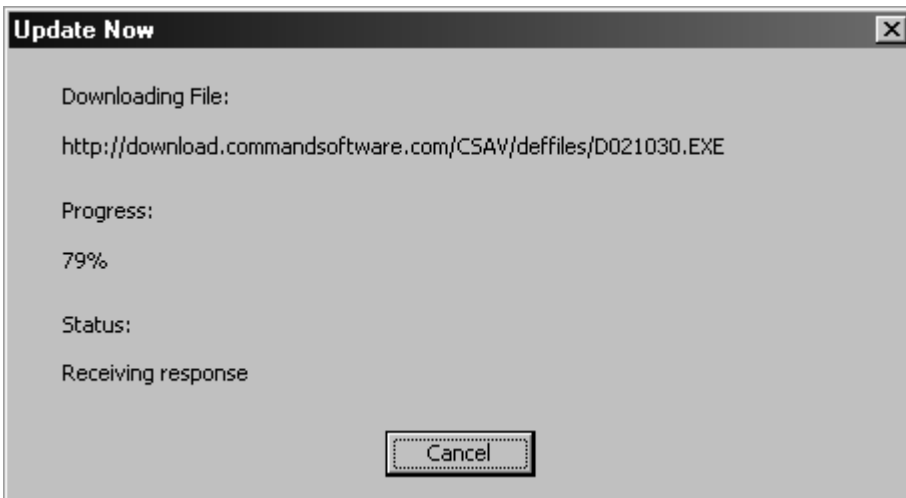
- **If you selected an ftp site** – the system displays the following **Enter Network Password** dialog box:



Enter Network Password Dialog Box – FTP Site

This dialog box does **not** display again as long as your user name and password remain valid.

6. In the **User Name** text box, type your Command user name.
7. In the **Password** text box, type your Command password.
8. Click **OK**. The system displays the **Update Now Download Status** dialog box:



Update Now Download Status Dialog Box

This dialog box identifies the file that is being downloaded and shows the progress and the status of the download.

9. When the download is complete, the installation begins. 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.



NOTE: If a problem occurs during the installation, the system displays an **Installation Error** message box.

CHECKING FOR UPDATES AUTOMATICALLY

To help you keep your Command AntiVirus software up-to-date, the **Update Now** feature allows you to set Command AntiVirus to notify you when virus definition file updates, component updates, and/or product upgrades are available. It also allows you to download and install virus definition file and component upgrades automatically.



NOTE: To use the **Update Now** feature, your computer **must** be connected to the Internet.

Before you can use the **Update Now** feature to check for updates and/or upgrades automatically, you need to set up **Update Now** in the **Preferences/Update Now** dialog box.



In Windows NT, Windows 2000, and Windows XP, this menu item is available **only** if you are signed on as a member of the Administrators group on the local machine.

The **Update Now** dialog box allows you to select:

- The site from which you want to download the files
- The updates and/or upgrades that you want to download
- Whether or not you want to be notified. This option allows you to specify the type of notification:



An update or upgrade is available to be downloaded



An update or upgrade has been downloaded and is ready to be installed

Automatically download and install without notification. This option is available **only** for virus definition file and component updates.

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

- **Sites** – Allows you to select the site from which you download the updated files. This dialog box also allows you to specify your Command AntiVirus user name and password for the download site and for any proxy server that you may use.
- **Updates** – Allows you to set Command AntiVirus to check for virus definition file updates, component updates, and/or product upgrades automatically. This dialog box also allows you to select whether or not you want to be notified when updated files are available.

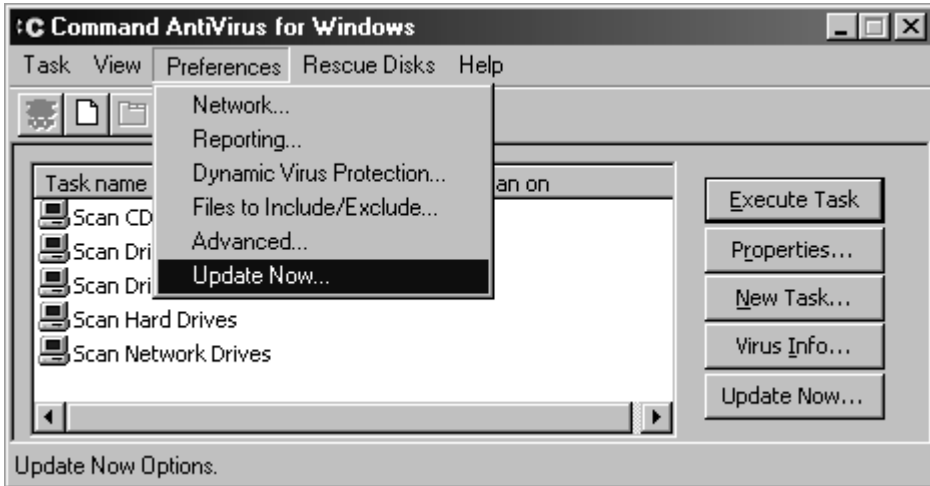


NOTE: For the **Update Now** feature to check for updates and/or upgrades automatically, you **must** provide the appropriate information in **both** the **Sites** and the **Updates** dialog boxes.

Setting Up the Notification Process

To set Command AntiVirus to check for updates and/or upgrades automatically, follow these steps:

1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Preferences Menu

2. Click **Update Now**. The system displays the **Update Now Setup** dialog box with the **Sites** dialog box in view:



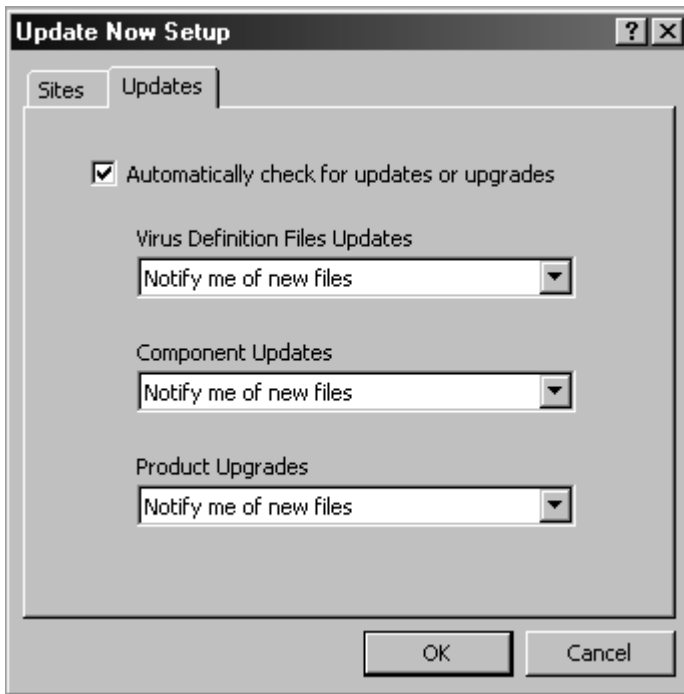
Sites Dialog Box

3. Under **Preferred Site**, click the drop-down arrow, and select a site for which you are authorized, for example, **USA http site**.
4. Click the **Site Credentials** button. The system displays the **Enter Network Password** dialog box:




Enter Network Password Dialog Box

5. In the **User Name** text box, type your Command user name.
6. In the **Password** text box, type your Command password.
7. Click **OK**. The system returns to the **Site** dialog box.
8. If you do **not** use a proxy server, go to **Step 9**.
If you do use a proxy server, click the **Proxy Credentials** button and repeat **Steps 5** through **7**.
9. Click the **Updates** tab. The system displays the **Updates** dialog box:



Updates Dialog Box


10. Select the **Automatically check for updates or upgrades** check box. This check box is selected by default.
11. Under **Virus Definition Files Updates**, click the drop-down arrow, and select **one** of the following:
 - **Notify me of new files** – Notifies you that there are new virus definition files available. This option is selected by default.

When new virus definition files are available, Command AntiVirus displays a **Download available** notification icon  in the Windows notification area. This option first requires that you start the download process, and then when you are ready, start the installation process.

For information on what to do when an **Update Now** notification icon is displayed, refer to **Understanding the Notification Messages** located later in this section.



NOTE: To see a ToolTip that identifies the function of the icon, move the mouse pointer over the icon.

- **Download new files and then inform me** – Downloads the latest virus definition files, and then Command AntiVirus displays an **Update ready for install** notification icon  in the Windows notification area. This option requires that you start the installation process.

For information on what to do when an **Update Now** notification icon is displayed, refer to **Understanding the Notification Messages** located later in this section.



NOTE: To see a ToolTip that identifies the function of the icon, move the mouse pointer over the icon.

- **Automatically download and install** – Downloads and installs the latest virus definition files without any notification.







NOTE: The **Automatically download and install** option is available **only** for virus definition file and component updates.

12. Repeat **Step 11 for Component Updates and Product Upgrades**.
13. Click **OK**. The system returns to the **Command AntiVirus Main** dialog box.

Command AntiVirus is now set to check for updates and/or upgrades automatically. For information on what to do when an **Update Now** notification icon is displayed in the Windows notification area, refer to **Understanding the Notification Messages** located later in this section.


Understanding the Notification Messages

When you set the **Update Now** feature to check for updates and/or upgrades automatically, Command AntiVirus displays **Update Now** notification icons in the Windows notification area to let you know the current state of the notification, for example:

- **Download available** icon 
- **Downloading** icon 
- **Download error** icon 
- **Update ready to install** icon 




NOTE: To see a ToolTip that identifies the function of an icon, move the mouse pointer over the icon.

The type of **Update Now** notification icon that Command AntiVirus displays first depends upon the options that you select in the **Preferences/Update Now/Updates** dialog box. For example, if you select the **Notify me of new files** option, Command AntiVirus first displays the **Download available** icon  in the Windows notification area.

For information on what to do when you receive an **Update Now** icon, refer to the section on the appropriate icon.



Download available

If you select the **Notify me of new files** option in the **Updates** dialog box, Command AntiVirus displays the **Download available** icon  in the Windows notification area when an update and/or upgrade is available to be downloaded.

The icon remains in the notification area until the download is started or the program that displays the icons is stopped, for example, when you log off of your computer.



NOTE: If the program that displays the icons is stopped, the icon disappears until the following day when you log on to your computer.



In Windows 2000 and Windows XP, the system displays the following balloon ToolTip when the icon first appears:

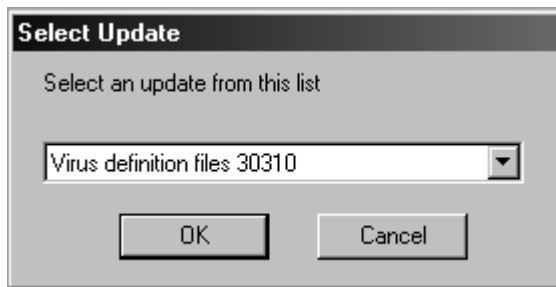


Download Available Balloon ToolTip

Starting the Download Process

To find out what type of update and/or upgrade is available and to start the download process, follow these steps:

1. In the Windows notification area, click the **Download available** icon . The system displays the **Select Update** dialog box:




Select Update Dialog Box



2. From the drop-down list, select the update or upgrade that you want to download. Available updates can include:
 - **Virus definition files** – Installs the latest virus definition files
 - **Update** – Installs the latest component update files
 - **CSAV X.XX.X** – Installs a full product upgrade of Command AntiVirus





NOTE: The x.xx.x represents the version number, for example, 4.80.0

3. Click **OK**. The download begins, and Command AntiVirus displays the **Downloading** icon  in the Windows notification area.




NOTE: You can cancel the download after it starts, by clicking the **Downloading** icon  and then clicking **Yes**. For more information, refer to  **Downloading** located later in this section.

If you receive a **Download error** icon , refer to  **Download error** located later in this section.

When the download is complete, Command AntiVirus displays the **Update ready to install icon**  in the Windows notification area. To start the installation, refer to  **Update ready to install** located later in this section.




Downloading

When an update and/or upgrade is downloading, Command AntiVirus displays the **Downloading** icon  in the Windows notification area. When the download begins, the ToolTip shows the percentage of the download that is complete.

The icon remains in the notification area until the download is finished or the program that displays the icons is stopped, for example, when you log off of your computer.




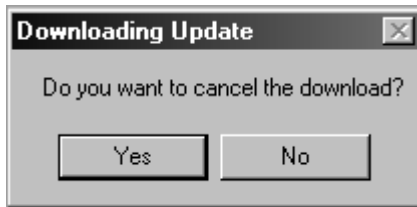
NOTE: If the program that displays the icons is stopped, the icon disappears until the following day when you log on to your computer.

When the download is complete, Command AntiVirus displays the **Update ready to install icon**  in the Windows notification area.

Canceling the Download Process

To cancel the download, follow these steps:

1. In the Windows notification area, click the **Downloading** icon . The system displays the **Downloading Update** dialog box:




Downloading Update Dialog Box

2. Click **Yes** to cancel the download.



Download error

When an error occurs in the download process, Command AntiVirus displays the **Download error** icon  in the Windows notification area.

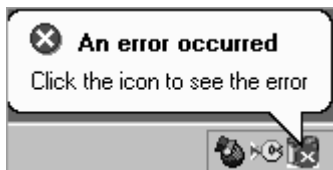
The icon remains in the notification area until you click the icon or the program that displays the icons is stopped, for example, when you log off of your computer.



NOTE: If the program that displays the icons is stopped, the icon disappears until the following day when you log on to your computer.




In Windows 2000 and Windows XP, the system displays the following balloon ToolTip when the icon first appears:

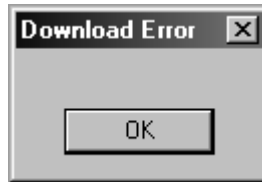


Download Error Balloon ToolTip

Understanding Why the Download Failed

To find out why the download process failed, follow these steps:

1. In the Windows notification area, click the **Download error** icon . The system displays the **Download error** message box:



Download Error Message Box

This message box contains an explanation of why download failed.

If the error is an Internet connection error, the system displays the **Connection Error** message box:



Connection Error Message Box


This message box asks that you check the following:

- Your Internet connection
- The site that you selected
- Your user name and password for the selected site

2. Click **OK** to exit the message box.



Update ready to install

If you select the **Download new files and then inform me** option in the **Updates** dialog box, or select to download available files from the **Select Update** dialog box, Command AntiVirus displays the **Update ready to install** icon  in the Windows notification area when an update and/or upgrade is available to be installed.

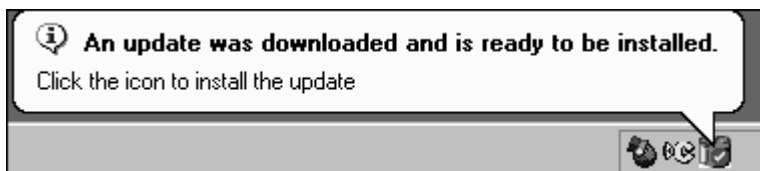
The icon remains in the notification area until the installation is started or the program that displays the icons is stopped, for example, when you log off of your computer.



NOTE: If the program that displays the icons is stopped, the icon disappears until the following day when you log on to your computer.




In Windows 2000 and Windows XP, the system displays the following balloon ToolTip when the icon first appears:

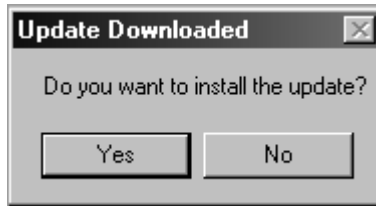


Update Ready To Install Balloon ToolTip

Starting the installation process

To start the installation, follow these steps:

1. In the Windows notification area, click the **Update ready to install** icon . The system displays the **Update Downloaded** dialog box:



Update Downloaded Dialog Box

2. Click **Yes**. The installation begins. 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.

CREATING A NEW SCAN TASK

Although Command AntiVirus comes with preset scan tasks for the most common tasks, you may want to create a special scan task to scan a particular drive, path, folder, or types of files. You can create this special scan task by first creating a new scan task from the **Task** menu and then setting the scan task properties in the **Properties** dialog box.

This section contains information on how to create a new scan task. For more information on setting the properties of a scan task, refer to **Setting Scan Task Properties** located in the next section.

To create a new scan task from the **Task** menu, follow these steps:

1. On the Command AntiVirus menu bar, click **Task**. The system displays the **Task** menu:

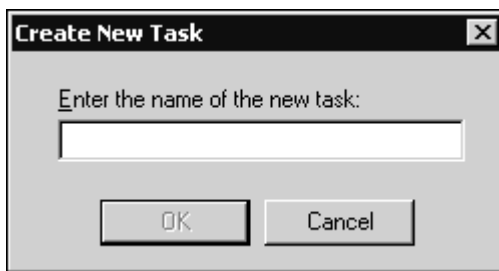


Task Menu

2. Click **New**. The system displays the **Create New Task** dialog box.



In Windows NT, Windows 2000, and Windows XP, if you are signed on as a member of the Administrators group on the local machine, the system first displays the **Select New Task Type** dialog box. Select the type of task, and click **OK**.




Create New Task Dialog Box

3. In the text box, type a name for your new task.
4. Click **OK**. The system displays the **Properties – Name of Scan Task** dialog box with the **Properties** dialog box in view.

You can either accept the default settings or customize the settings to your needs. For more information, refer to **Setting Scan Task Properties** located in the next section.



NOTE: To create a new task, 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.

SETTING SCAN TASK PROPERTIES

Although Command AntiVirus comes with preset scan tasks for the most common tasks, you may want to create a special scan task to scan a particular drive, path, folder, or types of files. You can create this special scan task by first creating a new scan task from the **Task** menu and then setting the scan task properties in the **Properties** dialog box for that scan task.

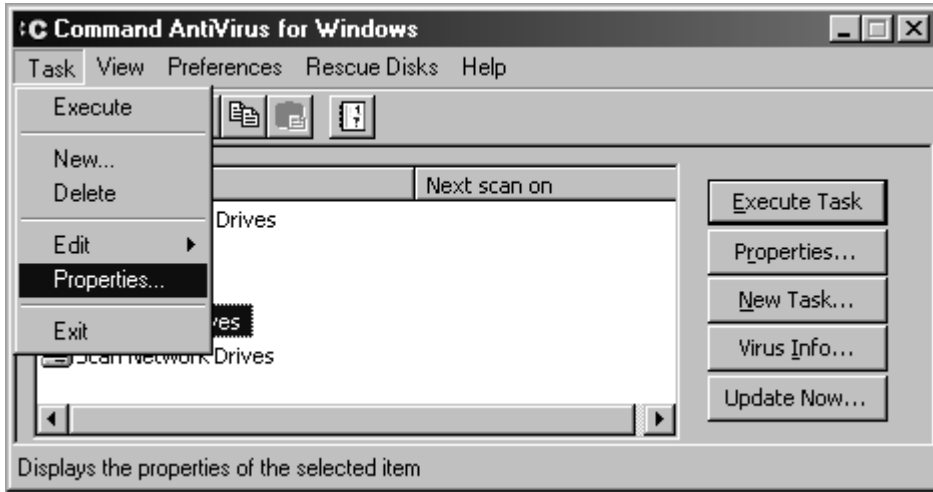
The **Properties – Name of Scan Task** dialog box contains the **Properties** and **Advanced Properties** dialog boxes that allow you to set the scanning properties of a scan task. Each of these dialog boxes are identified by a name tab.

In the **Properties** dialog box, you can select the **Paths/Drives to scan** and the **Action on infection** when a virus infection is found. In the **Advanced Properties** dialog box, you can select the **File types to scan**.

This section contains information on how to set the properties of a new or existing scan task.

To set the scanning properties of a scan task, follow these steps:


1. From the **Task List** in the **Command AntiVirus Main** dialog box, select a **Task name**.
2. On the Command AntiVirus menu bar, click **Task**. The system displays the **Task** menu:

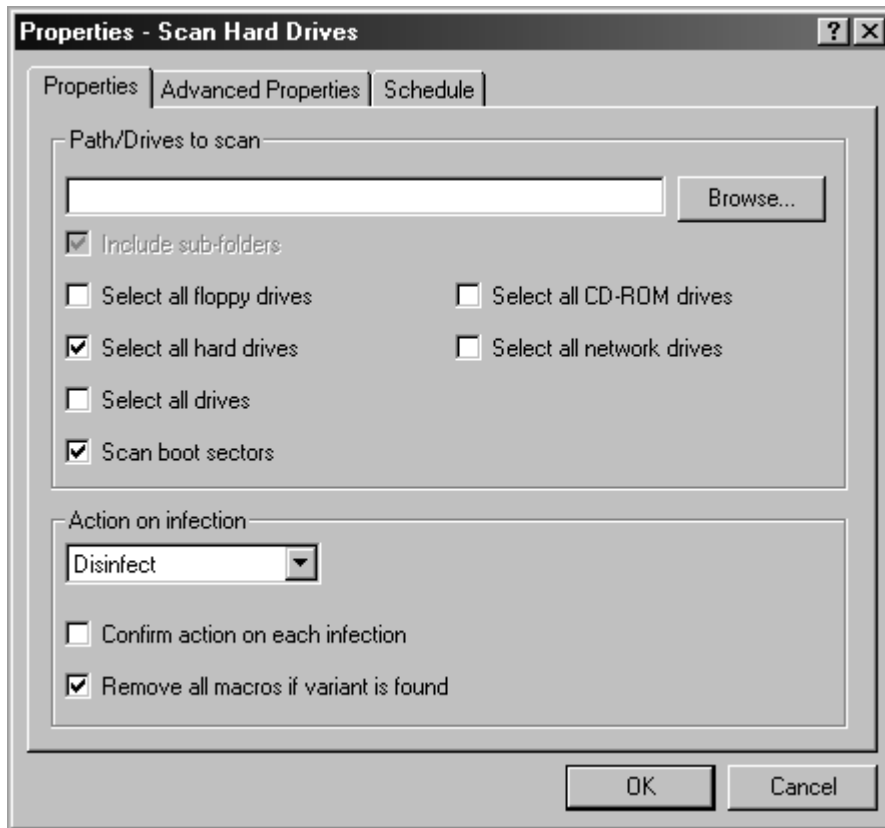


Task Menu

3. Click **Properties**. The system displays the **Properties – Name of Scan Task** dialog box with the **Properties** dialog box in view.



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.



Properties Dialog Box

4. Under **Path/Drives 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.



NOTE: Selecting a UNC path is **not** available for scheduled scans.

When you enter a path in the **Path/Drive 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. This option is selected by default.
 - **Select all drives** – Scans all drives to which you have access rights. This option is not available for scheduled scans.
 - **Scan boot sectors** – Scans the boot sectors of all logical hard drives on the local workstation including compressed drives. This option is selected by default.
 - **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 scans.
- 5. Under **Action on infection**, click the drop-down arrow. The system displays a drop-down list.
- 6. Select one of the following actions to take when a virus infection is found:
 - **Report** – Informs you when a virus infection is detected. No other action is taken. For example, you can select **Report** to verify the type of virus before disinfecting it.
 - **Delete** – Automatically deletes virus-infected files. If deletion is not possible, Command AntiVirus defaults to **Report**.



With **Delete**, the potential exists for data loss. Some rare virus infections are able to 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**. If renaming is not possible, Command AntiVirus defaults to **Report**.
- **Disinfect** – Automatically disinfects virus-infected files. If disinfection is not possible, Command AntiVirus defaults to **Quarantine**. This option is the default for all new scan tasks and for all of the preset scan tasks provided by Command AntiVirus.

Selecting the **Disinfect** 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. **Remove all macros if variant is found** is selected by default.



NOTE: If the **Action on infection** is **Disinfect** 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 only reported.



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

- **Quarantine** – Automatically adds a **.QUARANTINED** to the original file name and extension of the infected file. For example, **EICAR.COM** becomes **EICAR.COM.QUARANTINED**. CSAV then places the infected file in a separate folder for evaluation, disinfection or deletion at a later time.

If the quarantine folder does not have enough room to store the infected file, the file is not moved into that folder. Instead, the file is only reported by Command AntiVirus.

For more information, refer to **Using the Quarantine Feature** located later in this chapter.



In Windows NT, Windows 2000, and Windows XP, the **Quarantine** option is available only if you are signed on as a member of the Administrators group on the local machine.

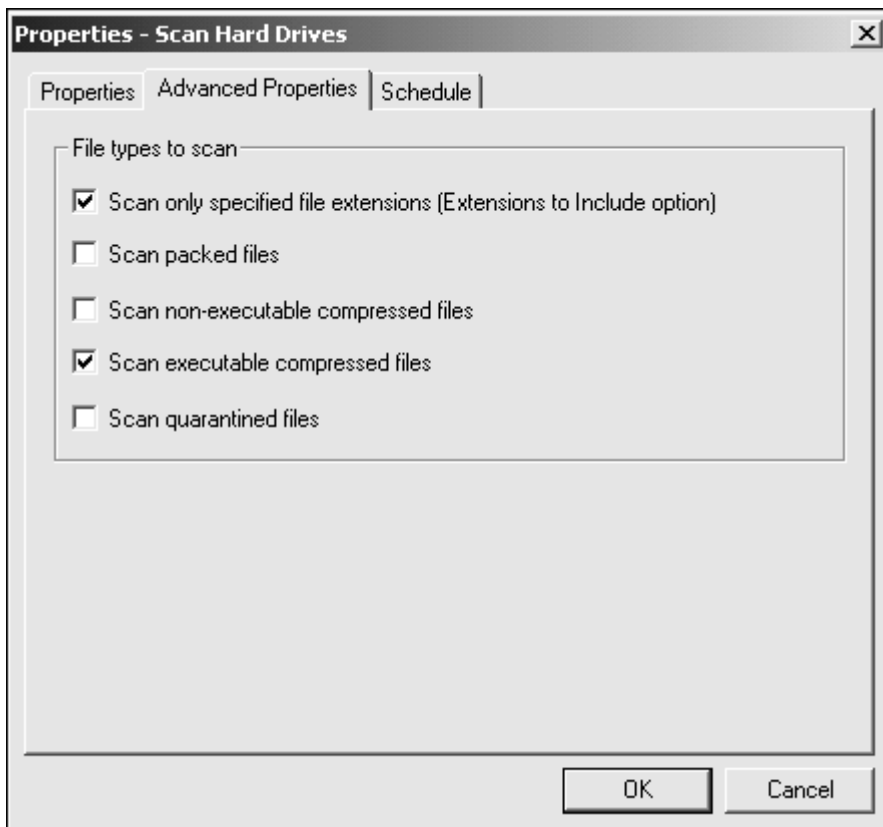


NOTE: If you want to be prompted before the selected action is taken on each infection, select the **Confirm action on each infection** check box.



Confirming the action on each infection is **not** available in scheduled scans as these scans usually occur unattended. If you selected the **Confirm action on each infection** check box, you are **not** prompted.

7. Click the **Advanced Properties** tab. The system displays the **Advanced Properties dialog box**:



Advanced Properties Dialog Box

8. Under **File types to scan**, select one or more of the following options:
- **Scan only specified file extensions (Extensions to Include option)** – Scans the default file types. Command AntiVirus contains “hard-coded” file types that are scanned by default. This option is selected by default.

You can also specify user-defined file types through the **Files to Include/Exclude** dialog box. For more information, refer to **Specifying Files/Directories To Scan** located later in this chapter.



NOTE: We recommend selecting **Scan only specified file extensions (Extensions to Include option)**.



If **Scan only specified file extensions (Extensions to Include option)** is **not** selected, CSAV scans **all** files including packed, non-executable compressed, and executable compressed files.

We do **not** recommend scanning **all** files. This type of scan 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.

- **Scan packed files** – Scans executable programs that have been compressed with programs such as ICE-packed, DIET, LZEXE-packed, PKLITE, or WWPack.
- **Scan non-executable compressed files** – Scans non-executable files that have been archived using programs such as PKWare’s ZIP and ARJ compression utilities.
- **Scan executable compressed files** – Scans executable files that have been archived using programs such as PKWare’s ZIP compression utility. This option is selected by default.

- **Scan quarantined files** – Scans 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 later in this chapter.

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



In Windows NT, Windows 2000, and Windows XP, the **Scan quarantined files** option is available only if you are signed on as a member of the Administrators group on the local machine.



NOTE: If the **Action on infection** is **Quarantine**, **Scan quarantined files** is unavailable as you **cannot** quarantine files that are already in the quarantine folder.

9. Click **OK**.

COPYING A SCAN TASK

You can create special scan tasks quickly and easily without resetting all of the scan task settings by copying a scan task that already exists and then specifying the drive, path, or folder to scan. You can copy a selected scan task from the **Task/Edit** menu, and then specify the path in the **Properties** dialog box.

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



In Windows NT, Windows 2000, and Windows XP, if you are **not** signed on as a member of the Administrators group on the local machine, you **cannot** cut a **System Task**.

If you are signed on as a member of the Administrators group on the local machine and you copy and paste a **System Task**, the task remains a **System Task**.

If you are **not** signed on as a member of the local Administrators group and you copy and paste a **System Task**, the task is converted to a **User Task**. It is then subject to the same restrictions that are associated with the assigned permissions.

This section contains information on how to copy a scan task. For more information on setting the properties of a scan task, refer to **Setting Scan Task Properties** located previously in this chapter.

To copy a scan task, follow these steps:

1. From the **Task List** in the **Command AntiVirus Main** dialog box, select the name of the scan task that you want to copy, for example, **scan hard drives**.
2. On the Command AntiVirus menu bar, click **Task**. The system displays the **Task** menu:



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.



NOTE: 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 **Setting Scan Task Properties** located previously 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.

DELETING A SCAN TASK



In Windows NT, Windows 2000, and Windows XP, if you are **not** signed on as a member of the Administrators group on the local machine, you **cannot** delete a **System Task**.

This section contains information on how to delete a scan task.

To delete a scan task, follow these steps:

1. From the **Task List** in the **Command AntiVirus Main** dialog box, select the name of the task that you want to delete.
2. On the Command AntiVirus menu bar, click **Task**. The system displays the **Task** menu:



Task Menu

3. Click **Delete**.



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

SETTING ON-ACCESS SCANNING PROPERTIES

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

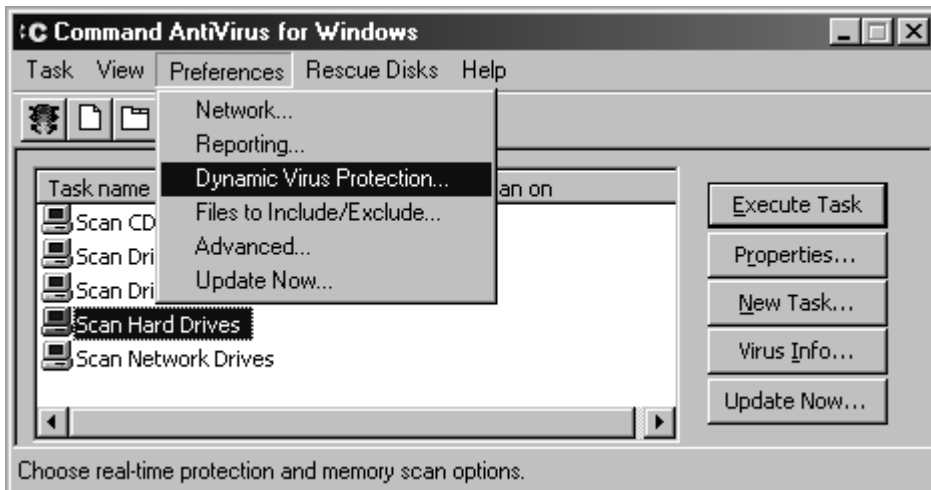
DVP provides transparent, on-access scans of each program that is run or file that is opened. This includes programs run from the hard drive, a diskette, or CD-ROM, and the boot sector of each diskette that is read. The moment you place a diskette or CD-ROM in the drive and run or copy a program, the diskette or CD-ROM is scanned automatically. DVP also scans files that are opened from the Command Prompt.

DVP is turned on by default and is set to disinfect when a virus infection is found. You can turn off DVP protection or change its on-access scanning properties through the **Preferences** menu. For example, you can select whether to scan diskette drives, local hard drives, or network drives. You can also select the action to take when a virus infection is found.

This section contains information on how to start or stop DVP scanning. It also contains information on how to set the DVP scanning properties.

To start or stop DVP scanning or change the DVP scanning properties, follow these steps:

1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Preferences Menu

2. Click **Dynamic Virus Protection**. The system displays the **Dynamic Virus Protection** dialog box:



Dynamic Virus Protection Dialog Box

3. Select or clear the **Enable Dynamic Virus Protection** check box. This option is selected by default.



This check box **must** be selected for on-access protection to work. We highly recommend that you select this option.

If you are disabling **Dynamic Virus Protection**, click **OK** to save your changes.

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

Enabling **Dynamic Virus Protection** activates this option. You can then select which types of drives are covered by DVP's on-access protection when files are accessed. The following options are selected by default:

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

5. Under **Action on infection**, click the drop-down arrow to select any **one** of the following actions to take when a virus infection is found.



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

- **Report** – Informs you when a virus infection is detected. No other action is taken other than to deny access to the file. For example, you can select **Report** to verify the type of virus before disinfecting it.
- **Delete** – Automatically deletes virus-infected files. If disinfection is not possible, Command AntiVirus defaults to **Report**.



With **Delete**, the potential exists for data loss. Some rare virus infections 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**. If renaming is not possible, Command AntiVirus defaults to **Report**.
- **Disinfect** – Automatically disinfects virus-infected files. If disinfection is not possible, Command AntiVirus defaults to **Report**. This option is selected by default.

Selecting the **Disinfect** 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. **Remove all macros if variant is found** is selected by default.



NOTE: If the **Action on infection** is **Disinfect** 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 only reported.



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

- **Quarantine** – Automatically adds a **.QUARANTINED** to the original file name and extension of the infected file. For example, **EICAR.COM** becomes **EICAR.COM.QUARANTINED**. CSAV then places the infected file in a separate folder for evaluation, disinfection or deletion at a later time.

If the quarantine folder does not have enough room to store the infected file, the file is not moved into that folder. Instead, the file is only reported by Command AntiVirus.

For more information, refer to **Using the Quarantine Feature** located later in this chapter.



In Windows NT, Windows 2000, and Windows XP, the **Quarantine** option is available only if you are signed on as a member of the Administrators group on the local machine.

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

SPECIFYING FILES/DIRECTORIES TO SCAN

Command AntiVirus contains a list of common file types that are scanned by default. This list is displayed in the **Included Extensions** list of the **Extensions to Include** dialog box. You cannot delete these “hard-coded” file types, but you can exclude a “hard-coded” file type from scans. For more information, refer to **Specifying Files to Exclude From Scans** located later in this section.

You can add to this list of scanned file types by specifying additional user-defined file types that you want CSAV to scan. You can also specify specific files and/or directories that you do **not** want CSAV to scan.

The **Preferences** menu allows you to set these file/directory settings. The **Files to Include/Exclude** option allows you to specify additional file types to **Include** in and what files and/or directories to **Exclude** from all scans.

The **Files to Include/Exclude** dialog box contains three dialog boxes: **Extensions 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: 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.

This section contains information on:

- Adding user-defined file types to the list of file types that CSAV scans
- Specifying files that you do **not** want CSAV to scan
- Specifying directories that you do **not** want CSAV to scan

ADDING ADDITIONAL FILE TYPES TO SCAN

Although Command AntiVirus contains a list of common file types that are scanned by default, you may want to add additional user-defined file types to scan. For example, you may have a software program that creates files with an extension that is not scanned by default. You can add this extension to the **Included Extensions** list of the **Extensions to Include** dialog box.



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

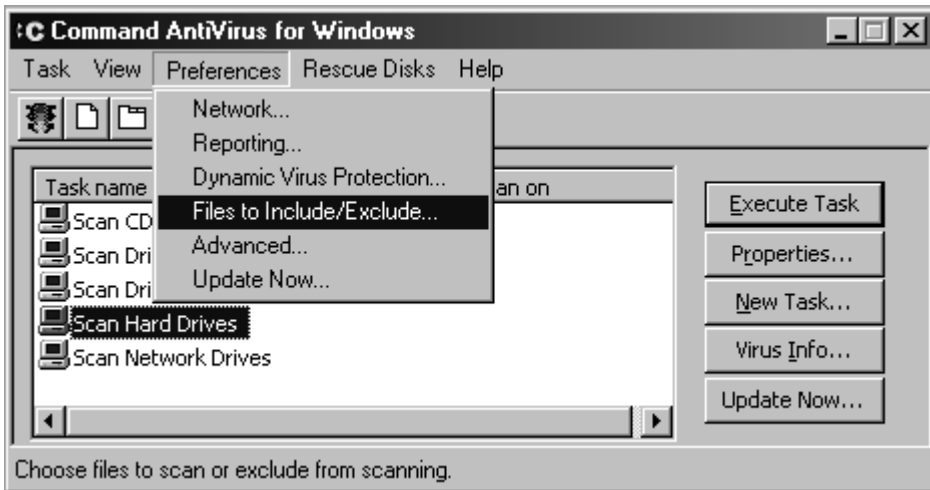
To scan the contents of self-extracting files in compressed form, we recommend that you perform an on-demand or scheduled scan of packed files during off-peak hours. To scan self-extracting and packed files, select the **Scan packed files** check box in the **Properties/Advanced Properties** dialog box.



NOTE: Compressed files that contain virus infections, cannot be disinfected. They can only be deleted.

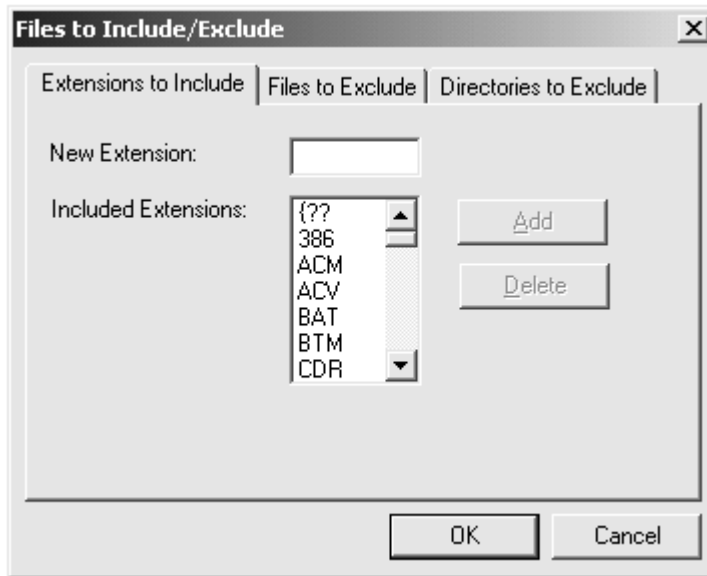
To add additional file name extensions to the list of file types CSAV scans, follow these steps:

1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Preferences Menu

2. Click **Files to Include/Exclude**. The system displays the **Files to Include/Exclude** dialog box with the **Extensions to Include** dialog box in view:



Extensions to Include Dialog Box

3. In the **New Extension** text box, type the extension that you want to add.
4. Click **Add**. The new extension is now in the **Included Extensions** list.



NOTE: To remove an extension that you have added, select the extension, and click **Delete**.

5. Click **OK** to exit the dialog box.

SPECIFYING FILES TO EXCLUDE FROM SCANS

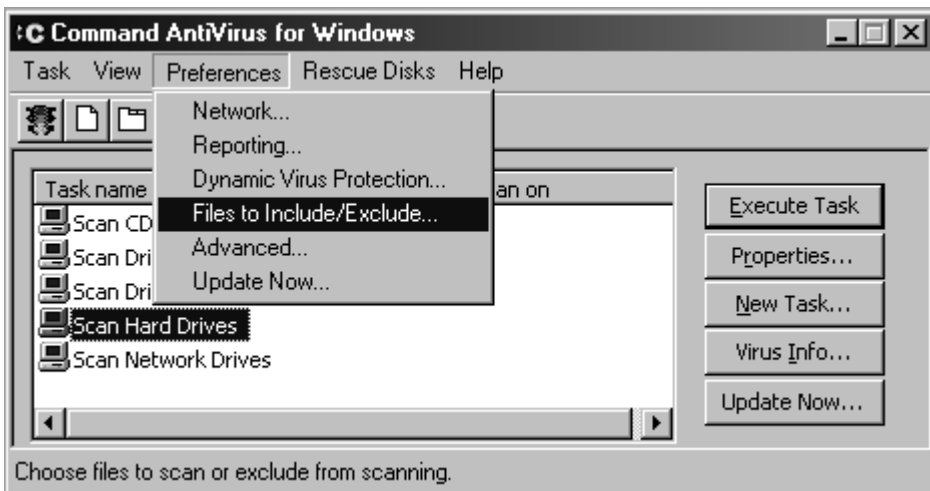
Although Command AntiVirus contains a list of common file types that are scanned by default, you may want to exclude specific files from being scanned. You can exclude files from being scanned by adding them to the **Excluded Filenames** list of the **Files to Exclude** dialog box.



As the potential of excluding files that may contain a virus infection exists, we recommend that you use this option with caution.

To add a file to the list of files that CSAV does **not** scan, follow these steps:

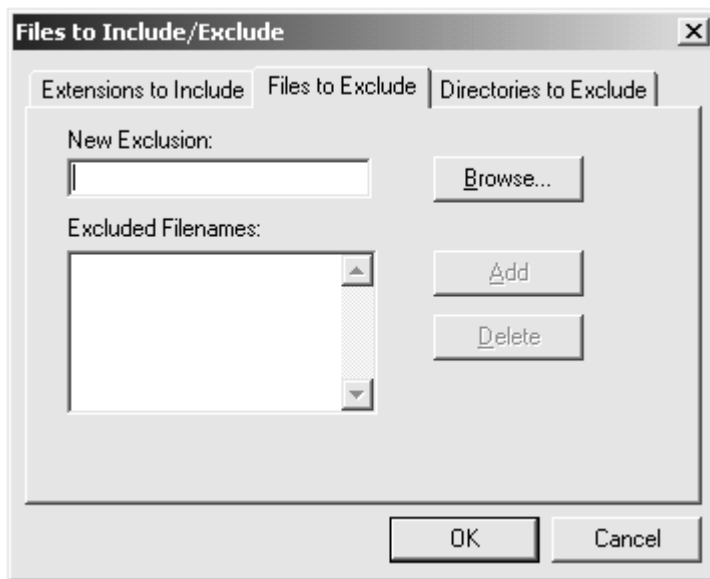
1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Preferences Menu

2. Click **Files to Include/Exclude**. The system displays the **Files to Include/Exclude** dialog box with the **Extensions to Include** dialog box in view.

- Click the **Files to Exclude** tab. The system displays the **Files to Exclude** dialog box:



Files to Exclude Dialog Box

- In the **New Exclusion** text box, type the full file name and extension or wildcard combination that you want to add.



NOTE: 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*



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

5. Click **Add**. The new file name is now in the **Excluded Filenames** list.



NOTE: To remove a file, select the file name from the list, and click **Delete**.

6. Click **OK** to exit the dialog box.

SPECIFYING DIRECTORIES TO EXCLUDE FROM SCANS

Although Command AntiVirus contains a list of common file types that are scanned by default, you may want to exclude specific directories from being scanned. You can exclude directories from being scanned by adding them to the **Excluded Directories** list of the **Directories to Exclude** dialog box.



As the potential of excluding directories that may contain a virus infection exists, we recommend that you use this option with caution.



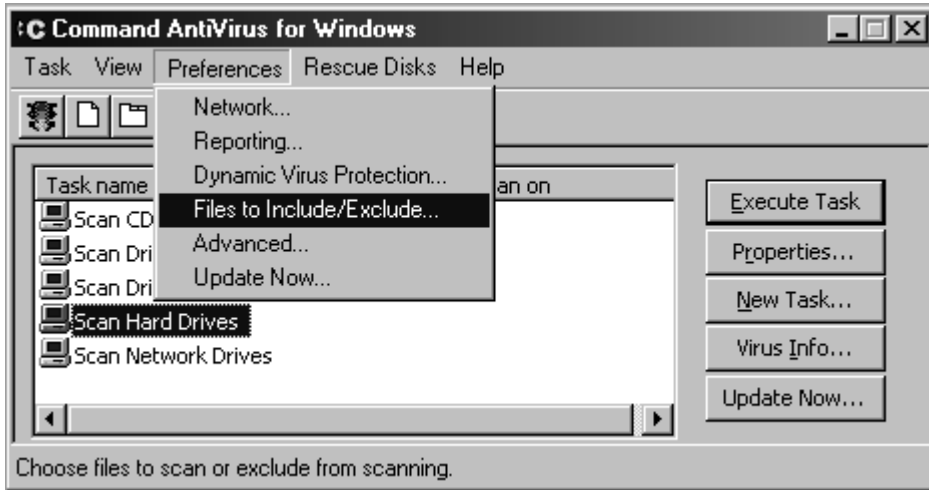
NOTE: When you exclude a directory, all of its subdirectories are excluded also. You **cannot** exclude just the specified directory.



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 of directories that CSAV does **not** scan, follow these steps:

1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Preferences Menu

2. Click **Files to Include/Exclude**. The system displays the **Files to Include/Exclude** dialog box with the **Extensions to Include** dialog box in view.
3. Click the **Directories to Exclude** tab. The system displays the **Directories to Exclude** dialog box:



Directories to Exclude Dialog Box

4. In the **New Exclusion** text box, type the directory name that you want to add.



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 **Add**. The new file name is now in the **Excluded Filenames** list.



NOTE: To remove a directory, select the directory from the list, and click **Delete**.

6. Click **OK** to exit the dialog box.

USING THE QUARANTINE FEATURE

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

To use this feature, you must first create a quarantine folder. The folder should be located on a local drive. For example, create a folder called **CSAV_quarantine** in the root of your C drive:

```
C:\CSAV_quarantine
```

Then, you must specify the path to the quarantine folder in the **Preferences/Advanced/Quarantine Path** dialog box. For more information refer to **Setting the Quarantine Path** located later in this section.

The quarantine option is available for files that are scanned using specific scan tasks (on-demand including scheduled) and for files scanned in real time through Dynamic Virus Protection (DVP). To move infected files to the quarantine folder automatically, you **must** set the **Action on infection** in the **Properties** dialog box of a task and/or in the **Dynamic Virus Protection** dialog box to **Quarantine**. For more information, refer to **Setting Scan Task Properties** and **Setting On-access Scanning Properties** located previously in this chapter.

When a file is moved to the quarantine folder, it is renamed by adding a **.QUARANTINED** extension to the file name. This action identifies the file as infected and quarantined.

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** becomes **Report**.
- If the **Action on infection** for an on-demand scan including scheduled scans is **Quarantine**, you **cannot** select **Scan quarantined files** located in the **Task/Properties/ Advanced Properties** dialog box.
- There are some items that you **cannot** quarantine. They are the Master Boot Record (MBR) and the boot sector. In these cases, the action taken by Command AntiVirus is **Report**.

- 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 is **not** the same. This is because the entire Zip file is quarantined.
- If DVP is active, you are 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 **Recycle Bin** and could be available to reinfect.



We recommend that you create a scan task setting the **Action on infection** to **Delete**. Then, run a scan on the quarantine folder to delete the infected files completely.

This section contains information on how to set the path to the quarantine folder and how to disinfect quarantined files.

Setting the Quarantine Path



In Windows NT, Windows 2000, and Windows XP, to perform this task, you **must** be signed on as a member of the Administrators group on the local machine.

In the **Quarantine Path** dialog box, you can set the path to the quarantine folder.



NOTE: You must first create a quarantine folder. The folder should be located on a local drive. For example, create a folder called **CSAV_quarantine** in the root of your C drive:

```
C:\CSAV_quarantine
```

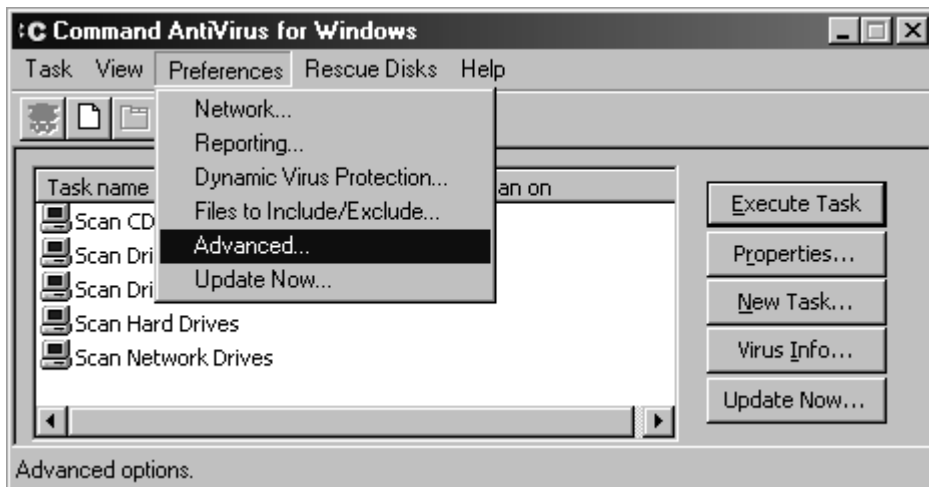
Infected files are routed to this folder only if you select the **Quarantine** option in the **Preferences/Dynamic Virus Protection** dialog box and/or the scan task's **Properties** dialog box. For more information, refer to **Setting Scan Task Properties** and **Setting On-access Scanning Properties** located previously in this chapter.



If you use this option to change the path to a different quarantine folder, files that were located in a previously defined quarantine folder will **not** be moved or modified.

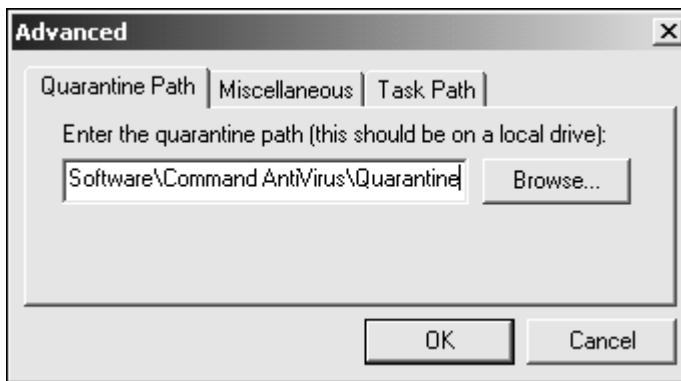
To set the path to the quarantine folder, follow these steps:

1. On the Command AntiVirus menu bar, click **Preferences**. The system displays **Preferences** menu:



Preferences 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:



Quarantine Path Dialog Box

4. In the **Enter the quarantine path** text box, type the full path to the 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**.

Disinfecting Quarantined Files

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



In Windows NT, Windows 2000, and Windows XP, the new task **must** be a **System Task**.

A user who is **not** signed on as a member of the Administrators group on the local machine can use this task as long as it was created as a **System Task** and access to the quarantine folder is permitted.

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

1. On the Command AntiVirus menu bar, click **Task**. The system displays the **Task** menu:



Task Menu

2. Select **New**. The system displays a **Create New Task** dialog box.

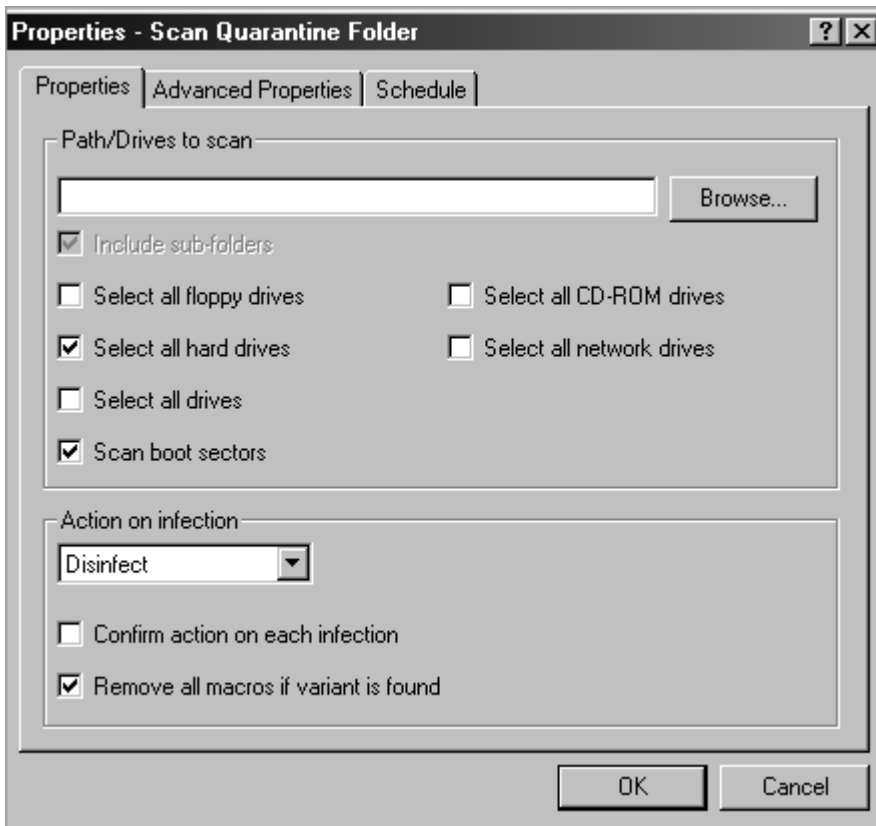


In Windows NT, Windows 2000, and Windows XP, if you are signed on as a member of the Administrators group on the local machine, the system first displays the **Select New Task Type** dialog box. Select **System**, and click **OK**.

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

Scan Quarantine Folder

4. Click **OK**. The system displays the **Properties – Name of Scan Task** dialog box with the **Properties** dialog box in view:



Properties Dialog Box

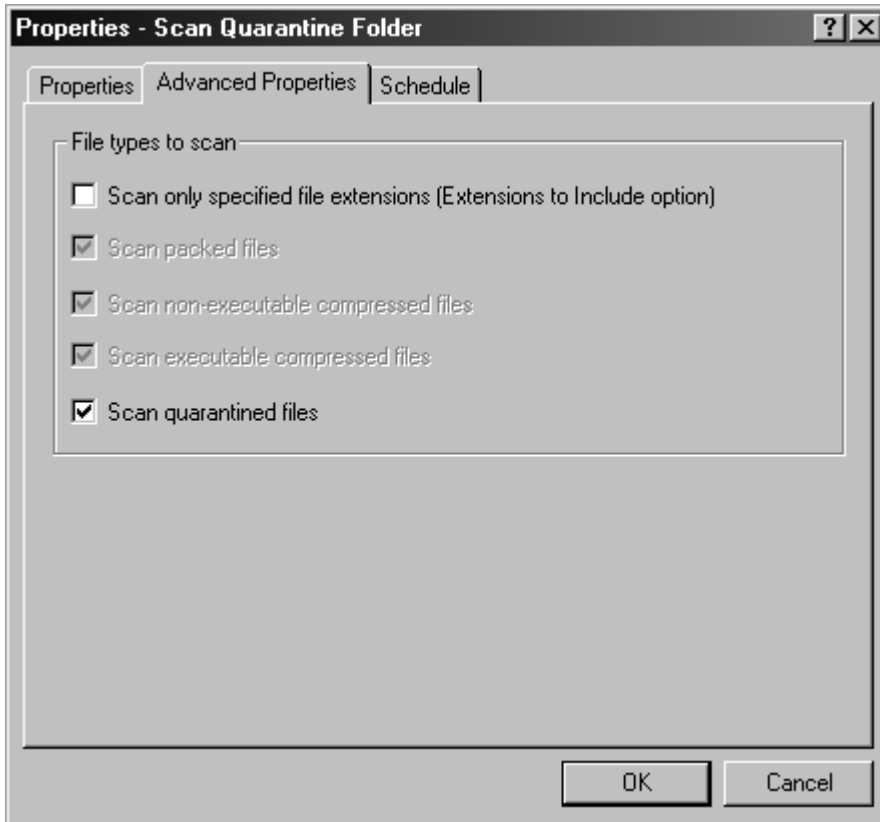
5. In the **Path/Drives to scan** text box, type the path to the quarantine folder.



NOTE: You can use the **Browse** button to select the path.

6. Under **Action on infection**, select **Disinfect**.

- Click the **Advanced Properties** tab, the system displays the **Advanced Properties** dialog box:



Advanced Properties Dialog Box

- Under **File types to scan**, clear the **Scan only specified file extensions (Extensions to Include option)** to select all files.
- Select the **Scan quarantined files** check box.
- Click **OK**. The system returns to the **Command AntiVirus Main** dialog box.

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 are disinfected, you **must** rename the files to their original names and move the files back to their original locations.



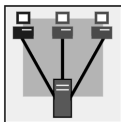
NOTE: If for some reason a file was **not** disinfected and DVP is active, you are stopped if you try to copy or move an infected file.



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 on infection** 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 **Recycle Bin** and could be available to reinfect.

SENDING A VIRUS NOTIFICATION MESSAGE



Administrators can set Command AntiVirus to mail a virus report when a virus infection is found to a recipient, for example, the Administrator, using an existing SMTP (Simple Mail Transfer Protocol) e-mail system. You can set this e-mail option through the **Preferences/Reporting** dialog box.



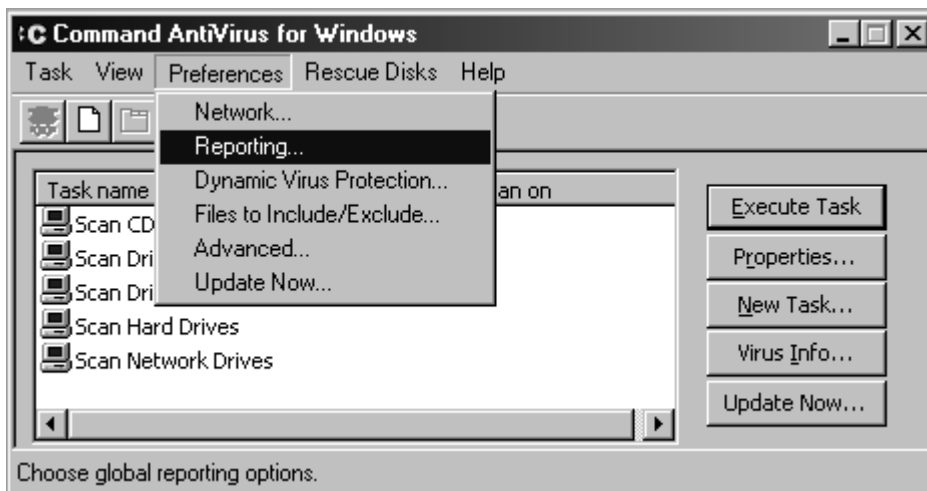
NOTE: As you can send a virus report at the end of a manual scan, this **E-mail** option does **not** apply to manual scans.

For scheduled scans, a single report is mailed at the end of the scan. For on-access scanning, a report is mailed each time a virus infection is found.

This section contains information on how to send a virus notification message when a virus infection is found.

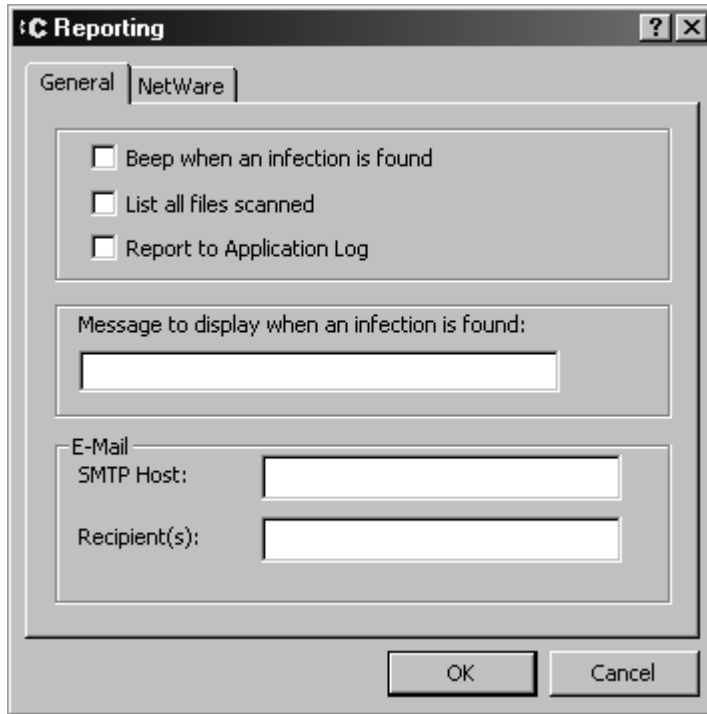
To set up sending a virus notification e-mail, follow these steps:

1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Preferences Menu

2. Click **Reporting**. The system displays the **Reporting** dialog box with the **General** dialog box in view:



General Dialog Box

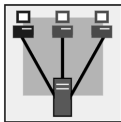
3. Under **E-Mail**, in the **SMTP Host** text box, type the name of the local SMTP host.
4. In the **Recipient(s)** text box, type who receives the messages, for example, Administrator.



NOTE: You can specify multiple recipients by typing a semicolon (;) between each recipient.

5. Click **OK**.

SETTING UP VIRUS REPORTING TO A NETWARE SERVER



Administrators can set Command AntiVirus to log virus infections found to a NetWare server. If a virus infection is found, it is added to the Command AntiVirus for NetWare log file on the server that you specify. To view the log, use a text editor or the **View** option in the **Command AntiVirus for NetWare Administration Main** dialog box.

You can set this logging option through the **Preferences/Reporting/NetWare** dialog box.



NOTE: To use this option, you **must** have Command AntiVirus for NetWare installed on a Novell® NetWare® server.

You must also have the Command AntiVirus for Windows **NetWare Reporting** feature installed and running. If **NetWare Reporting** is **not** installed and running, the **Preferences/Reporting/NetWare** dialog box is **not** visible.

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

The **NetWare Reporting** feature is **not** installed by default. You must install this feature during installation or afterwards by using the installation program's **Application Maintenance** dialog box. For more information on installation, refer to the **Installation** chapter of this guide.



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

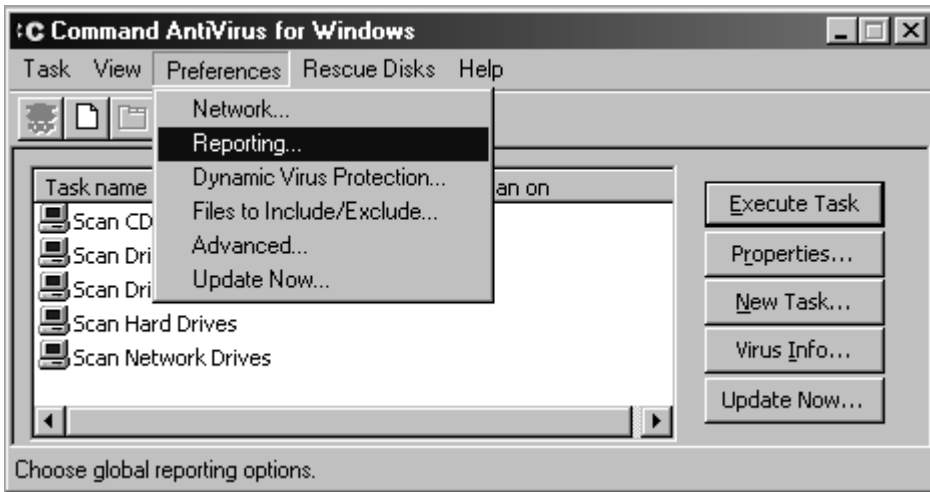
This section contains information on how to log virus infections found to a NetWare server.



NOTE: This logging option does **not** apply to manual scans.

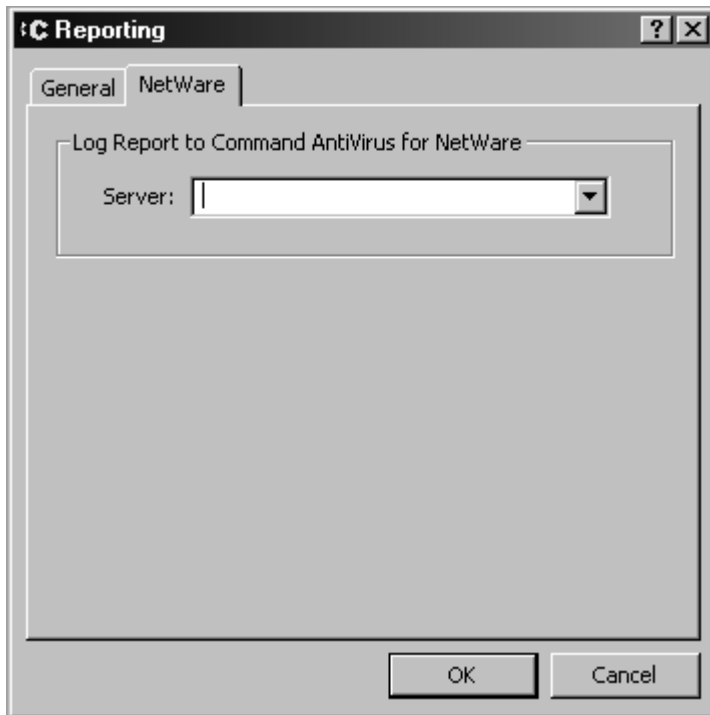
To set up logging virus infections to a Command AntiVirus for NetWare log file on a NetWare server, follow these steps:

1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Preferences Menu

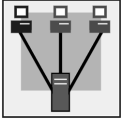
2. Click **Reporting**. The system displays the **Reporting** dialog box with the **General** dialog box in view.
3. Click the **NetWare** tab. The system displays the **NetWare** dialog box:



Reporting - NetWare Dialog Box

4. Under **Log Report to Command AntiVirus for NetWare**, in the **Server** text box, type a valid server name, or select a valid server name from the drop-down list.
5. Click **OK**.

SETTING CSAV SCANNING OPTIONS FOR NETWARE DRIVES



Administrators can specify how Command AntiVirus behaves when scanning a network drive that has NetWare installed. For example, you can preserve the last access date on the file being scanned. You can also skip compressed files and/or migrated files from being scanned.

You can set these scanning options through the **Preferences/Network** dialog box.

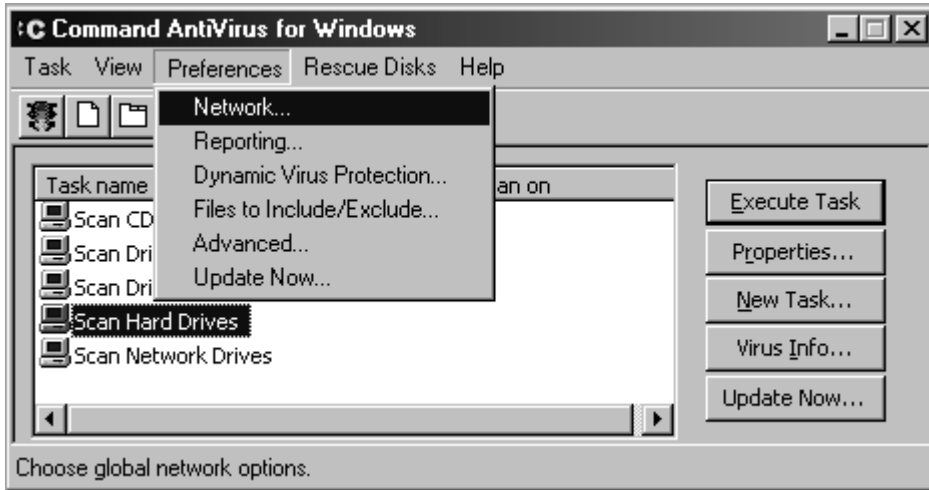


NOTE: The **Network** menu item is available **only** if you have the Novell® NetWare® client installed.

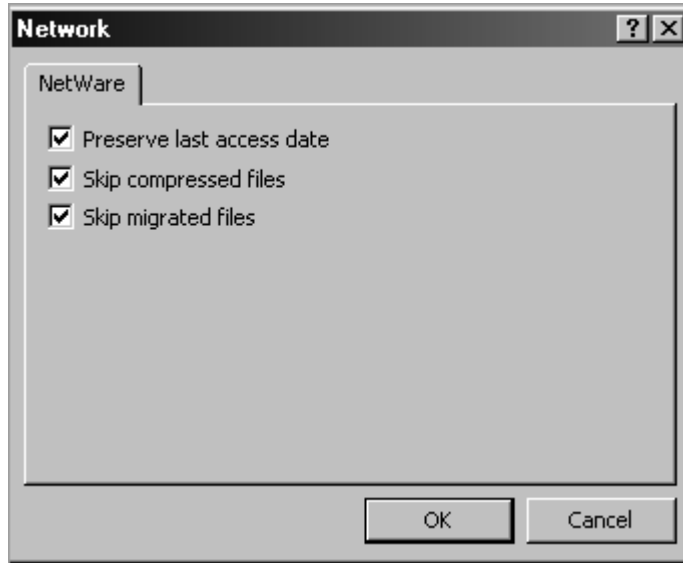
This section contains information on how to set scanning options for NetWare drives.

To set the scanning options for NetWare drives, follow these steps:

1. From the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:

**Network Dialog Box**

2. Click **Network**. The system displays the **Network** dialog box with the **NetWare** dialog box in view:



Network - NetWare Dialog Box

3. Select any of the following options:

- **Preserve last access date** – Prevents the modification of the last access date on the file. This option is selected by default.

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. This option is selected by default.

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 infection.

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. This option is selected by default.

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.

4. Click **OK**.

CHANGING THE SYSTEM SCAN TASK FOLDER

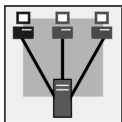


In Windows NT, Windows 2000, and Windows XP, to perform this task, you **must** be signed on as a member of the Administrators group on the local machine.

The preset scan tasks that come with Command AntiVirus and the additional Command AntiVirus **System Tasks** that you create, by default, are stored in a Windows folder on your hard drive.



NOTE: Scan task files always use an **.FPT** extension. For more information on **System Tasks**, refer to **Task Window** located previously in this chapter.

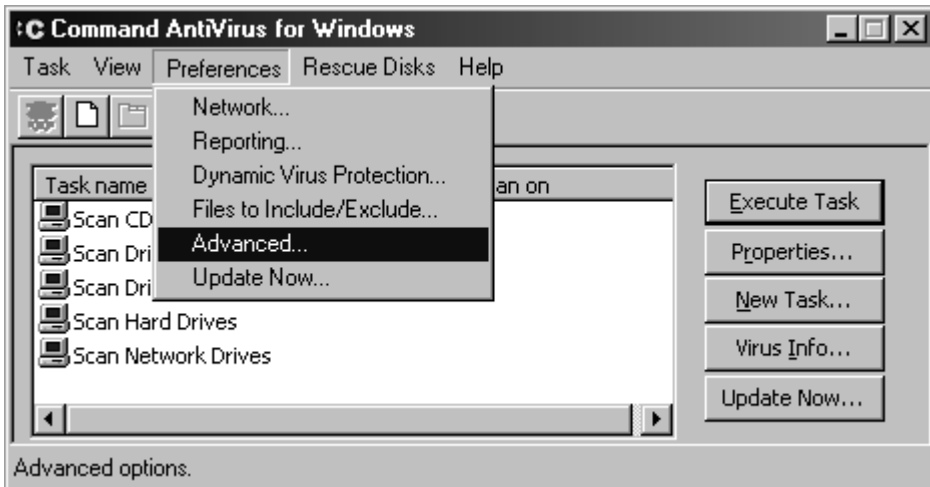


As a network administrator, you may want to change the folder that stores system scan tasks. For example, you may want to create a set of specific scan tasks for your users that are stored in a network folder to which they have access. You can specify the new path in the **Preferences/Advanced/Task Path** dialog box.

This section contains information on how to change the folder that contains the **System** scan tasks.

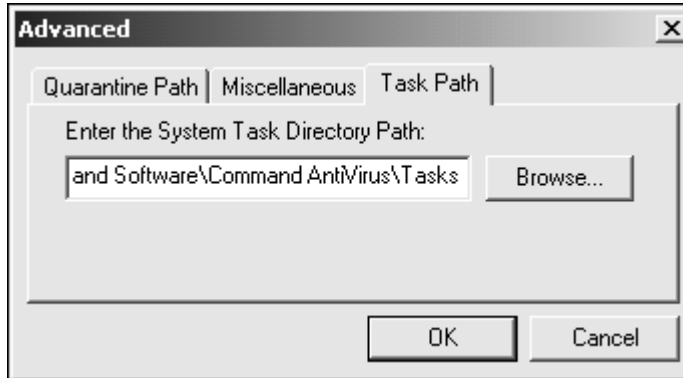
To change the default Command AntiVirus **System** scan task folder, follow these steps:

1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Preferences 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:



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 **System** scan tasks in the new location are now displayed in the **Command AntiVirus Main** dialog box.

SCANNING MAIL

Command AntiVirus includes a plugin for Microsoft Outlook® called the Outlook Scanner. The Outlook Scanner scans messages and attachments of incoming and outgoing mail for viruses. Unscanned mail is scanned and marked as scanned when it is opened.



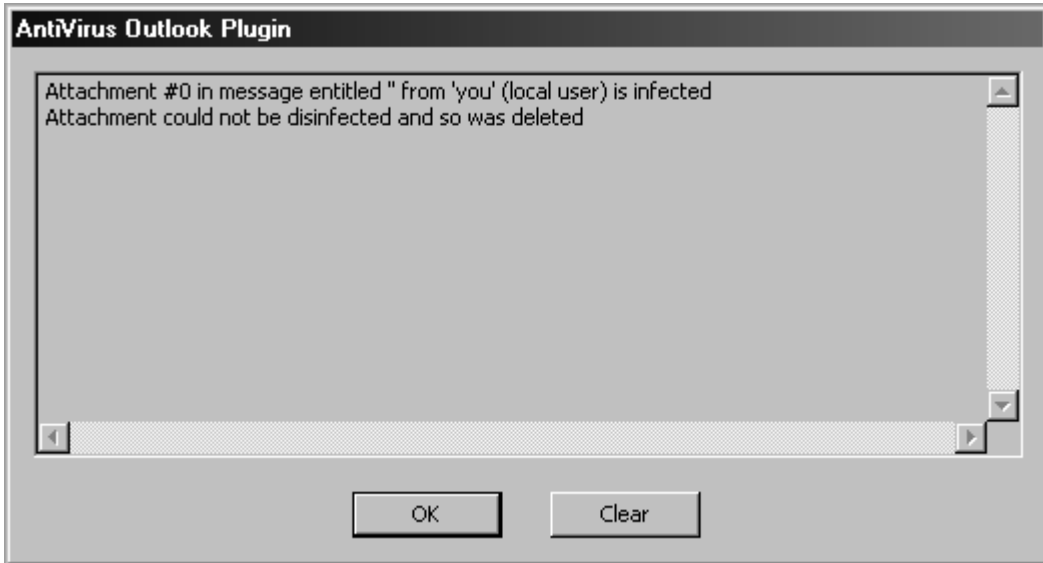
NOTE: The Outlook Scanner does **not** apply to Microsoft Outlook Express.

The Outlook Scanner is **not** installed by default. You must install this feature during installation or afterwards by using the installation program's **Application Maintenance** dialog box. For more information, refer to the **Installation** chapter of this guide.

This section contains information on how the Outlook Scanner works.

If you are logged into Microsoft Exchange client or Microsoft Outlook, the Outlook Scanner is at work when you send or receive infected e-mail messages. As soon as you receive an e-mail into your mailbox, click **Send** to send an e-mail, or open an unscanned e-mail, the Outlook Scanner scans the body and the attachments of the e-mail. This scan includes shortcuts to infected files, embedded files in the message, and embedded messages.

If a virus is found, the Outlook Scanner displays the **AntiVirus Outlook Plugin** dialog box:



AntiVirus Outlook Plugin Dialog Box

This dialog box provides the following information for **each** infected file that is found:

- Attachment Number
- E-mail Subject
- Sender's Name
- Status of the attachment, for example, disinfected or deleted



NOTE: All virus messages remain in the **AntiVirus Outlook Plugin** dialog box until you remove them by clicking the **Clear** button.

Click **OK** to exit.

GETTING HELP

You can find the answers to many of your product-related questions through the **Help** menu. For example, you can find information on

- a specific topic
- product enhancements, bug fixes, and special instructions
- how to contact your Technical Support representative
- viruses handled by Command AntiVirus
- product version
- virus definition files
- installation
- installed components

This section contains information on how to get the help that you need.

To access the **Help** menu, follow these steps:

1. On the Command AntiVirus menu bar, click **Help**. The system displays the **Help** menu:



Help Menu

2. Click the appropriate menu item.

The following topics will help you find the information that you need.

FINDING INFORMATION ON A SPECIFIC TOPIC

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

FINDING INFORMATION ON THE LATEST CHANGES

The **README.TXT** file contains the latest information on product enhancements, bug fixes, and special instructions for each release. To view this information, on the **Help** menu, click **Readme.txt**. This menu item opens the **Readme.txt** file.

CONTACTING A TECHNICAL SUPPORT REPRESENTATIVE

To find information on contacting your local technical support representative, on the **Help** menu, click **Technical Support**. This menu item provides telephone numbers and other information on Command AntiVirus contacts worldwide.

VIEWING A LIST OF VIRUSES HANDLED BY CSAV

To view a list of viruses handled by Command AntiVirus, on the **Help** menu, click **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 virus definition files that are on your computer.

VIEWING CSAV PRODUCT INSTALLATION INFORMATION

To view Command AntiVirus product installation information, on the **Help** menu, click **About**. This menu item provides information on the following topics.

Finding Version and Definition File Information

The **About Command AntiVirus for Windows** message box provides the following information:

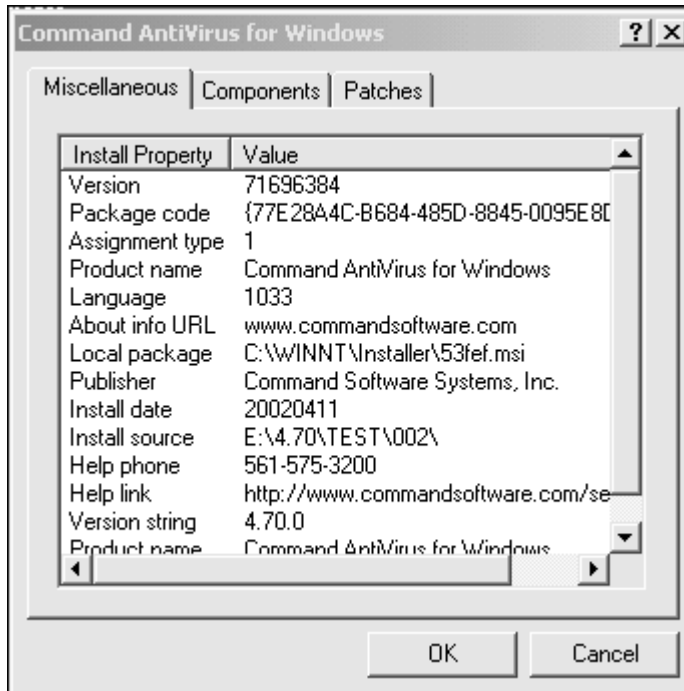
- Product version number
- Date of the scan engine
- Date of the **SIGN.DEF** definition file
- Date of the **SIGN2.DEF** definition file
- Date of the **MACRO.DEF** definition file
- Copyright information

Finding Product Installation Details

The **Details** button allows you to view additional data relating to the current version of the product, the components that make up the product, and any product patches that have been applied. It provides a source of information that can be helpful when you are troubleshooting a problem.

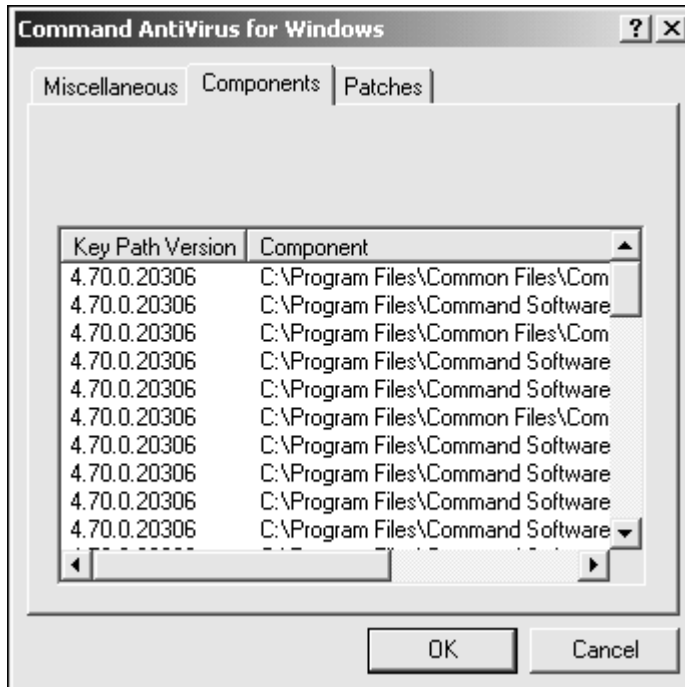
The **Details** dialog box contains three dialog boxes: **Miscellaneous**, **Components**, and **Patches**.

The **Miscellaneous** dialog box contains information that is specific to the currently installed version of the product. For example, it contains the name of the product, the date the product was installed, the location of the installation source, etc.:



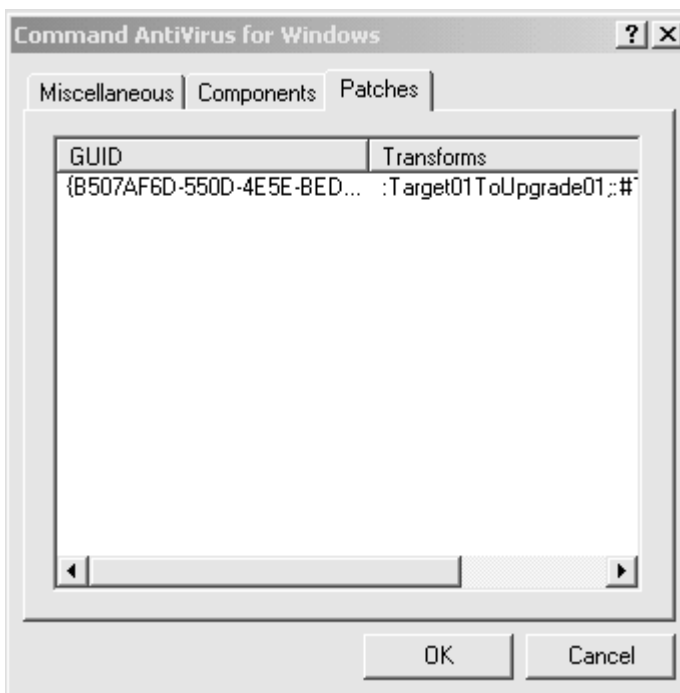
Miscellaneous Dialog Box

The **Components** dialog box contains the version number and the location of each installed component of the product:



Components Dialog Box

The **Patches** dialog box contains identifying information for each patch that is installed:



Patches Dialog Box



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 Virus Lab 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®, to create a rescue file, you must be a member of the Administrators group on the local machine.

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. The default directory is:

```
C:\PROGRAM FILES\COMMON FILES\COMMAND SOFTWARE
```

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. The default directory is:

```
C:\PROGRAM FILES\COMMON FILES\COMMAND SOFTWARE
```

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

Table 1: 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

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



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.

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

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

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

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

When the scan is complete, remove **Rescue Disk 3** from drive A.

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.

- Make sure that your computer's boot sector protection (Boot Sector Virus Protection) is turned **off**. Not all CMOS setups have this feature.

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 the boot sequence in CMOS has drive A selected as the initial boot drive, for example, A:, C:.

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 diskette for a copy of DOS, appearing to boot properly.

Make the necessary changes and complete the steps outlined in **Unknown Variant**. If these steps do not solve the problem, call your local technical support representative for further assistance.



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.



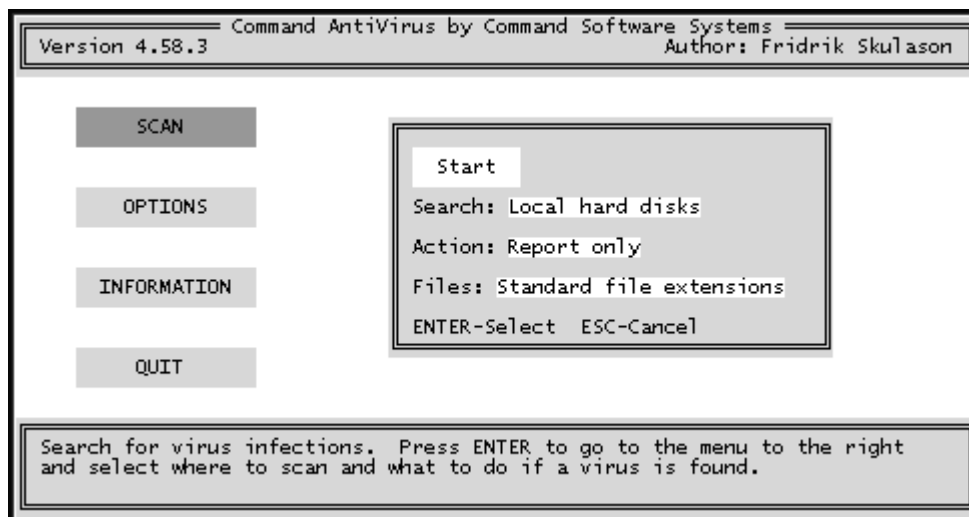
NOTE: For NTFS systems, unless you can access an NTFS drive from within DOS, for example, by using third party software, you will **not** be able to use the rescue disk set to scan files on an NTFS drive.

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:



Main Menu

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

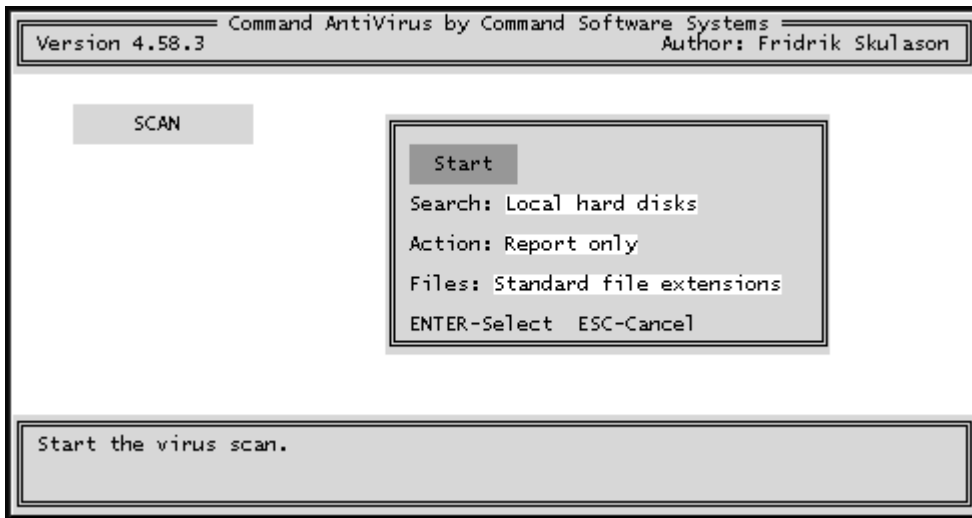


NOTE: When an item is selected, a description of the item appears in an information box at the bottom of the screen. From any screen, you can go back to the previous screen by pressing the **ESC** key.

The following section describes these items in detail.

SCAN

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



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.

```

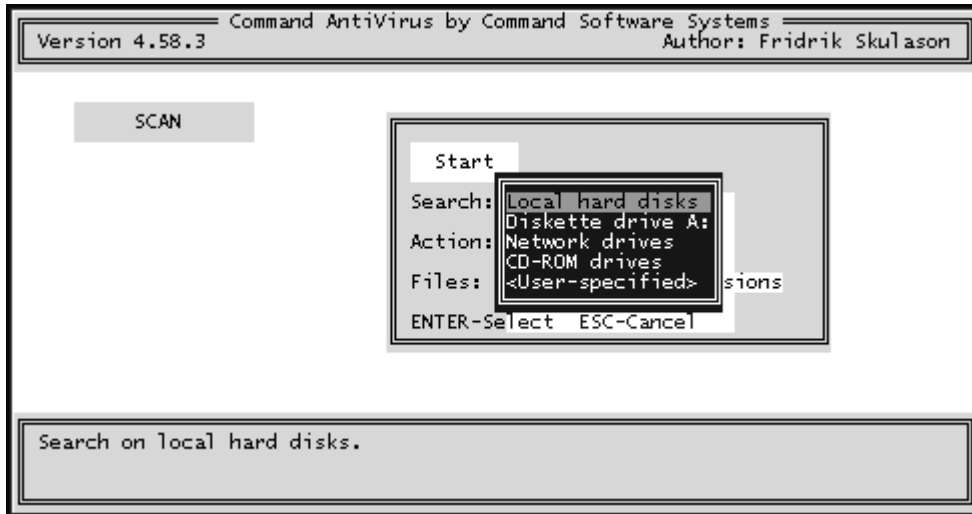
Files: Standard file extensions
Switches: <none>
No viruses found in memo
No viruses were found in
Scanning C:
C:\RECYCLED\DC250.COM I
C:\RECYCLED\DC253.EXE->E
C:\CDROMDRV\MSCDEX.EXE
Results of virus scannin
Files: 3276
MBRs: 1
Boot sectors: 1
Objects scanned: 3106
Infected: 2
Suspicious: 0
Disinfected: 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.
ESC-Cancel

```

Results of Virus Scanning

Search

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



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:



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 disinfecting. 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.

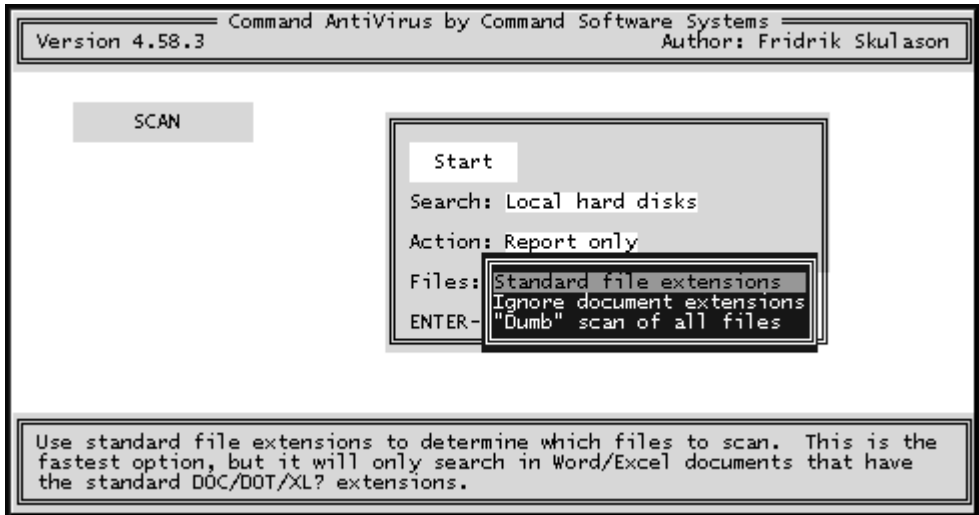
Use this option if you want study the infected file or compare it to a virus-free backup copy.

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:



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 antivirus 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

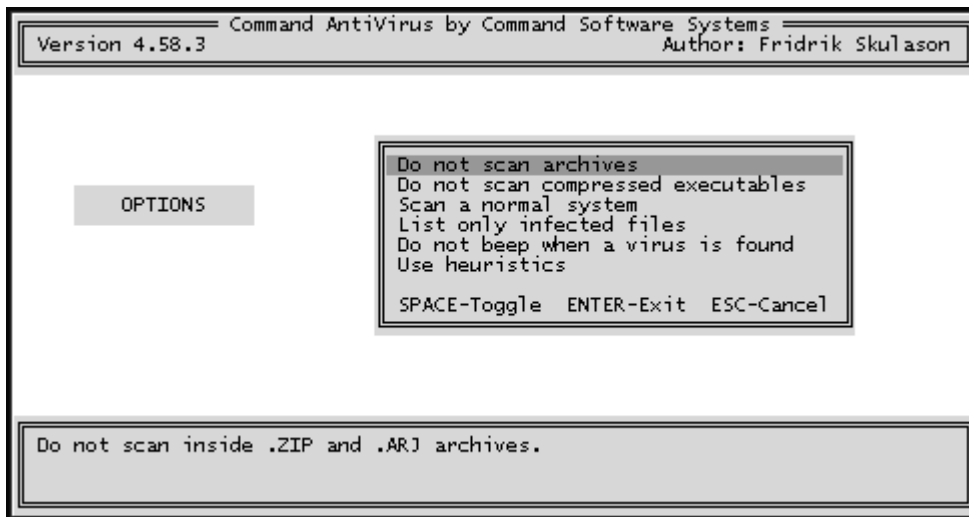


This option scans every file. We do not recommend this option for inexperienced users as scanning all files on a disk could produce a false indication of a virus. Use this option only if one of the following conditions exists:

- 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:



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

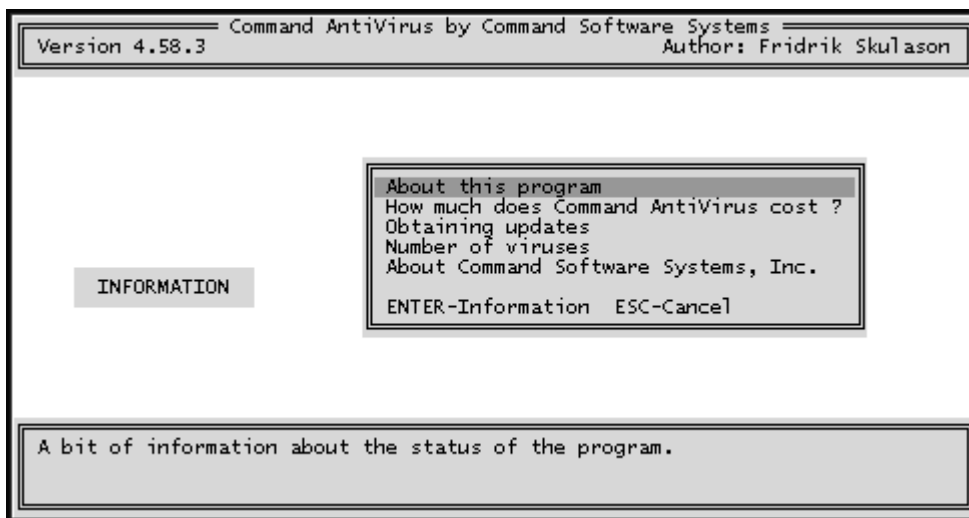
This option allows you to select the heuristics scanning method.



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:



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.
/INTER	Forces interactive mode.

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

Switch	Description
/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 <i>Network Administration</i> 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.
/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.

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

Switch	Description
/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.



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 memory in the computer 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 antivirus products. The EICAR test file is the result of a cooperative effort between various antivirus 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 antivirus 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 (refer to 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.

TUNNELING

A characteristic of some viruses that try to access the operating system directly, bypassing any TSRs (including antivirus 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 (refer to 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.

INDEX

A

- Action on infection
 - on-access scanning 3-91
 - on-demand scans 3-81
- Adding features 2-27

B

- Boot record support
 - creating a rescue file 4-1
 - disinfecting a boot sector virus 4-5
 - if disinfection fails 4-7
 - repairing 4-3

C

- Changing
 - task names 3-8
 - the Quarantine path 3-103
 - the System scan task folder 3-118
- Chapter overview 1-2
- Command AntiVirus
 - Main dialog box 3-3
 - accessing 3-19
 - command buttons 3-10
 - menu bar 3-12
 - Help menu 3-18
 - Preferences menu 3-15
 - Rescue Disks menu 3-17
 - Task menu 3-13
 - View menu 3-14
 - Shortcut menu 3-12
 - Task Window 3-5
 - changing task names 3-8
 - sizing columns 3-9
 - sorting order of scan tasks 3-8
 - Task List 3-5–3-6
 - types of scan tasks 3-7
 - updating information 3-9

- toolbar buttons 3-19
- main features 1-1
- Readme.txt file 1-9
- system requirements 1-6
- testing 1-7
- updating 3-55
 - automatically 3-61
 - notification messages 3-68
 - setting up 3-62
 - on-demand 3-55

Command Software

- Command-line utilities 4-1, 4-3, 5-1
- Mailing List Server 1-8
- technical support 1-8, 3-125, 5-8
- Web site 1-8

Conventions used 1-4

Copying a scan task 3-85

Creating a

- new scan task 3-76
- Rescue Disk set 2-19–2-23, 3-20–3-24
- rescue file 4-1

Custom installation (see Installation)

D

Deleting a scan task 3-88

Dynamic Virus Protection (DVP) (see on-access scanning)

F

Features

- adding 2-27
- removing 2-27

H

- Help menu 3-18, 3-123
 - installation information 3-125
 - latest changes 3-124

- list of viruses 3-125
- specific topic 3-124
- technical support 3-125

I**Installation**

- Custom 2-1, 2-3, 2-9–2-18
 - installation state 2-12–2-14
 - select features 2-11–2-12
- details 3-125
- maintenance 2-24
 - adding features 2-27
 - removing
 - CSAV 2-30
 - features 2-27
 - repairing 2-29
 - starting the program 2-25
- prerequisites 2-3
- state 2-12–2-14, 2-28
- system requirements 2-2
- Typical 2-1, 2-3, 2-4–2-9

M

- Mail scanning 3-2, 3-121
- Master Boot Record (MBR) (see Boot record support)

O

- On-access scanning 3-1
 - reporting 3-39
 - setting properties 3-89
 - starting and stopping 3-89
 - viewing scan results 3-40
 - from the View menu 3-41
 - in the Windows Event Viewer 3-45
- On-demand scan 3-1
 - customizing 3-49
 - reporting 3-27, 3-32
 - scheduling 3-35
 - setting properties 3-78
 - starting 3-25
 - from the command line 3-34

- from the Task menu 3-26
- from the Windows shortcut menu 3-33
- viewing scan results 3-40
 - from the View menu 3-41
 - in Windows Event Viewer 3-45

Q

- Quarantine feature
 - disinfecting quarantined files 3-105
 - setting the path 3-103
 - using 3-102

R

- Removing
 - CSAV 2-30
 - features 2-27
- Reporting
 - customizing 3-49
 - on-access 3-39
 - on-demand 3-27, 3-32
 - to a NetWare server 3-112
- Rescue Disk set 3-20
 - creating 2-19–2-23, 3-21–3-24
 - using 2-23–2-24, 3-24–3-25

S

- Scan tasks
 - changing names 3-8
 - copying 3-85
 - creating 3-76
 - deleting 3-88
 - setting properties 3-78
 - sorting order 3-8
 - System 3-6–3-7
 - changing the folder 3-118
 - User 3-7
- Scanning
 - directories to exclude 3-99
 - DOS-based 5-1
 - command-line mode 5-14
 - menu 5-2

- extensions to include 3-93, 3-94
 - files to exclude 3-97
 - mail 3-2, 3-121
 - on-access 3-1
 - reporting 3-39
 - setting properties 3-89
 - starting and stopping 3-89
 - viewing scan results 3-40
 - from the View menu 3-41
 - in the Windows Event Viewer 3-45
 - on-demand 3-1
 - reporting 3-27, 3-32
 - scheduling 3-35
 - setting properties 3-78
 - starting 3-25
 - from the command line 3-34
 - from the Task menu 3-26
 - from the Windows shortcut menu 3-33
 - viewing results 3-40
 - from the View menu 3-41
 - in the Windows Event Viewer 3-45
 - setting options for NetWare drives 3-115
 - Scheduling an on-demand scan 3-35
 - Setting
 - an audible virus warning 3-50
 - scanning options for NetWare drives 3-115
 - scanning properties
 - on-access 3-89
 - on-demand 3-78
 - virus reporting to a NetWare server 3-112
 - Starting
 - an on-demand scan 3-25
 - on-access scanning 3-89
 - System requirements 1-6, 2-2
- T**
- Technical support 1-8, 3-125, 5-8
 - Typical installation (see Installation)
- U**
- Uninstalling CSAV 2-30
 - Updating CSAV 3-55
 - automatically 3-61
 - notification messages 3-68
 - setting up 3-62
 - on-demand 3-55
 - Using a Rescue Disk set 2-23–2-24, 3-24–3-25
- V**
- Viewing scan results
 - from the View menu 3-41
 - in the Windows Event Viewer 3-45
 - Virus
 - boot sector 4-1
 - disinfecting 4-5
 - if disinfection fails 4-7
 - definition files
 - setting a warning 3-52
 - updating
 - automatically 3-55
 - on-demand 3-55
 - information 3-125
 - notification
 - mailing a virus report 3-110
 - receiving an infection warning 3-44
 - setting an audible warning 3-50
-