Command AntiVirus™

for

Windows® Enterprise

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

Administrator’s Guide

NOTICE

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

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

LICENSE AGREEMENT

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

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

For each License acquired, Licensee may use one copy of the Software on a "one user per license" basis, or in its place, any prior version for the same operating system, on a single computer. Licensee may also store or install a copy of the Software on a storage device, such as a network server, used only to install or run the Software on Licensee's other computers over an internal network; however, Licensee must acquire and dedicate a License for each separate computer on which the Software is installed or run from the storage device. A license for the Software may not be shared or used concurrently on different computers. A server License requires user access licenses on a "one user per access license" basis, or as defined with each server product.

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

WARRANTY

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

**Published in the U.S.A. by Command Software Systems, Inc. All rights reserved.
Document No. CW32A-480-0303**

Part No. 07-9200-00

TABLE OF CONTENTS

INTRODUCTION

This chapter provides an overview of Command AntiVirus for Windows® Enterprise including a list of product features, system requirements, and conventions used throughout this 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 Enterprise is a comprehensive antivirus 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® Enterprise Administrator'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 - NETWORK ADMINISTRATION

Chapter 6 contains information on what administrators need to do to prepare for the installation of Command AntiVirus for Windows Enterprise across the network.

For example, this chapter outlines the steps that you need to take to customize, install, update, and upgrade Command AntiVirus for Windows Enterprise quickly and easily.

CHAPTER 7 - COMMANDCENTRAL

This chapter provides information on our centralized management package called COMMANDCentral.

COMMANDCentral contains administrative tools that allow you to deploy the Command AntiVirus Pre-installation Convenience Pack onto machines across your network, customize features and settings prior to deploying CSAV, advertise CSAV across your network, and download Command AntiVirus updates and upgrades.

CHAPTER 8 - GLOSSARY

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

CONVENTIONS USED

⚠	Indicates an area that requires special attention.
✓	Indicates a helpful tip.
🖧	Indicates network-specific information.
NT	Indicates information that is specific to Windows NT.
2000/XP	Indicates information that is specific to Windows 2000/XP.
NT/2K/XP	Indicates information that is specific to Windows NT/2000/XP.
95/98/Me	Indicates information that is specific to Windows 95/98/Me.

`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 Enterprise, 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, or Microsoft Internet Explorer 4.01 and the Command AntiVirus Pre-installation Convenience Pack installed on each machine on which you want to install Command AntiVirus.

Windows 95 OSR2 machines that have Microsoft Internet Explorer 5.0 installed **must** also have the Command AntiVirus Pre-installation Convenience Pack installed.

The Command AntiVirus Pre-installation Convenience Pack is part of COMMANDCentral. COMMANDCentral also contains the Command AntiVirus Deployment Prep Wizard that can help you to install the prerequisite files across your network.

For more information on the wizard, refer to the ***COMMANDCentral*** chapter of this guide.

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® Enterprise 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

For information on administrative installation and deploying to multiple users over the network, refer to the ***Network Administration*** chapter of this guide.

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, or Microsoft Internet Explorer 4.01 and the Command AntiVirus Pre-installation Convenience Pack installed on each machine on which you want to install Command AntiVirus.

Windows 95 OSR2 machines that have Microsoft Internet Explorer 5.0 installed **must** also have the Command AntiVirus Pre-installation Convenience Pack installed.

The Command AntiVirus Pre-installation Convenience Pack is part of COMMANDCentral. COMMANDCentral also contains the Command AntiVirus Deployment Prep Wizard that can help you to install the prerequisite files across your network.

For more information on the wizard, refer to the ***COMMANDCentral*** chapter of this guide.

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.

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, **one** of the following conditions **must** be met:

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

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.

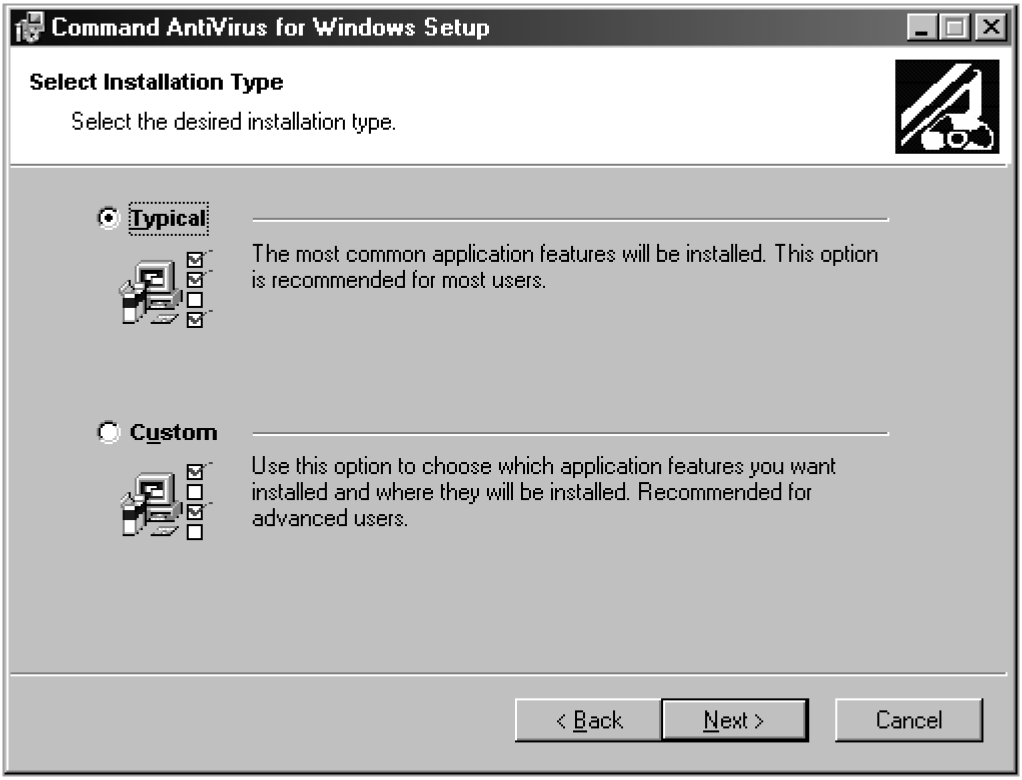
TYPICAL INSTALLATION

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:



Command AntiVirus for Windows Setup

Select Installation Type

Select the desired installation type.

● Typical

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

○ Custom

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

Select Installation Type Dialog Box

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 a dialog box informing you that Command AntiVirus for Windows has been successfully installed.

9. 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.

For information on updating your virus definition files across the network, refer to the ***Network Administration*** 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.

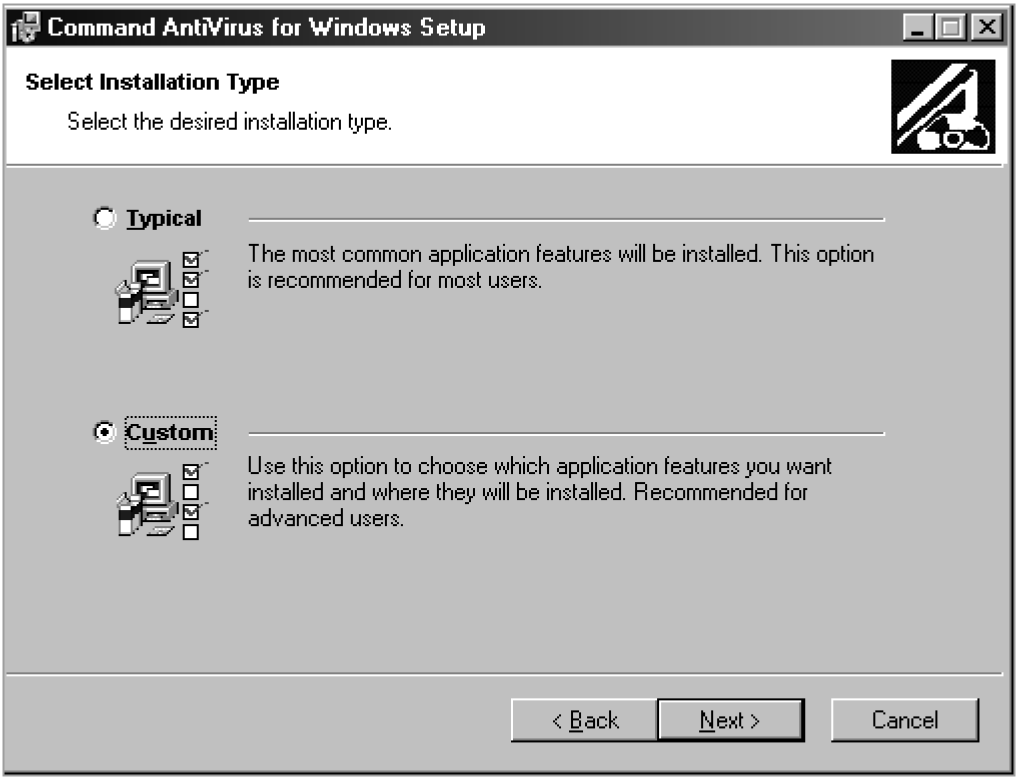
CUSTOM INSTALLATION

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

Select the desired installation type.

○ Typical

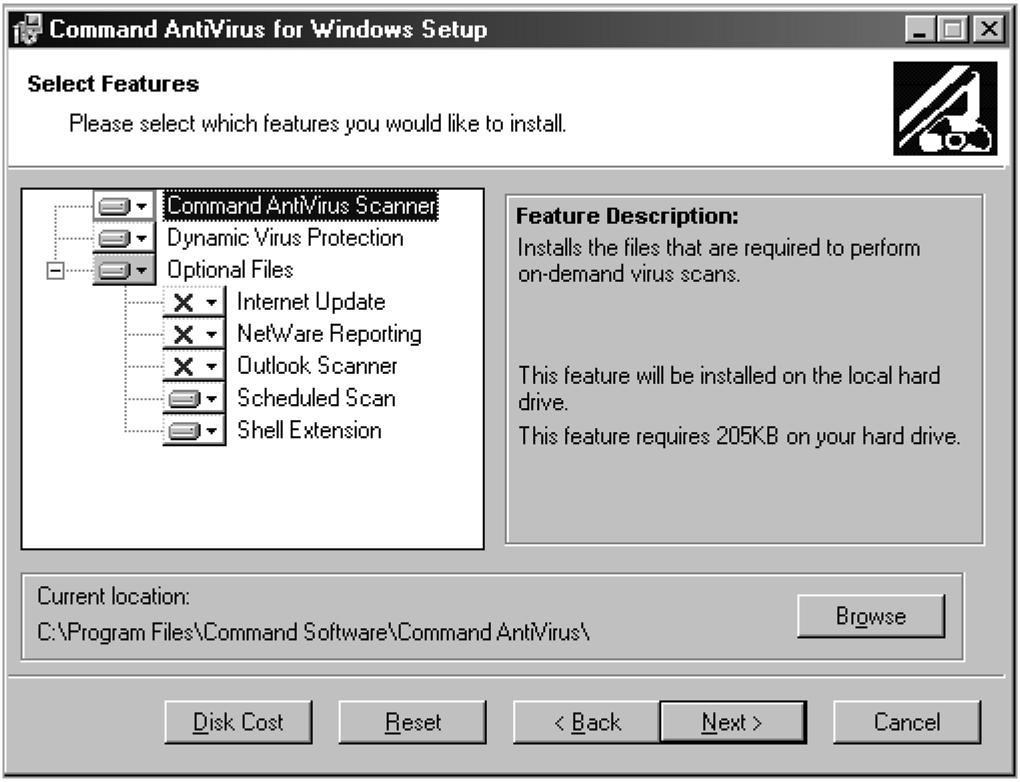
The most common application features will be installed. This option is recommended for most users.

● Custom

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

Select Installation Type Dialog Box

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


Command AntiVirus for Windows Setup
Select Features
Please select which features you would like to install.
Command AntiVirus Scanner
Dynamic Virus Protection
Optional Files
Internet Update
NetWare Reporting
Outlook Scanner
Scheduled Scan
Shell Extension
Feature Description:
Installs the files that are required to perform on-demand virus scans.
This feature will be installed on the local hard drive.
This feature requires 205KB on your hard drive.
Current location:
C:\Program Files\Command Software\Command AntiVirus\
Browse
Disk Cost
Reset
< Back
Next >
Cancel

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:

  - **Internet Update** – installs the files that are required to allow the end user to update virus definition files, components, and full product from the Internet. This subfeature is **not** installed by default.

NOTE: When you install the **Internet Update** feature, the Enterprise method of updating through an administrative image is replaced by updating through the Internet.

The **CSAV Update** button in the Command AntiVirus graphical user interface (GUI) is replaced by the **Update Now** button, and the **CSAV Update Setup** item on the **Preferences** menu is replaced by **Update Now**. For more information on updating CSAV, refer to **Updating Command AntiVirus** located in the ***Using Command AntiVirus*** chapter of this guide.

  - **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.

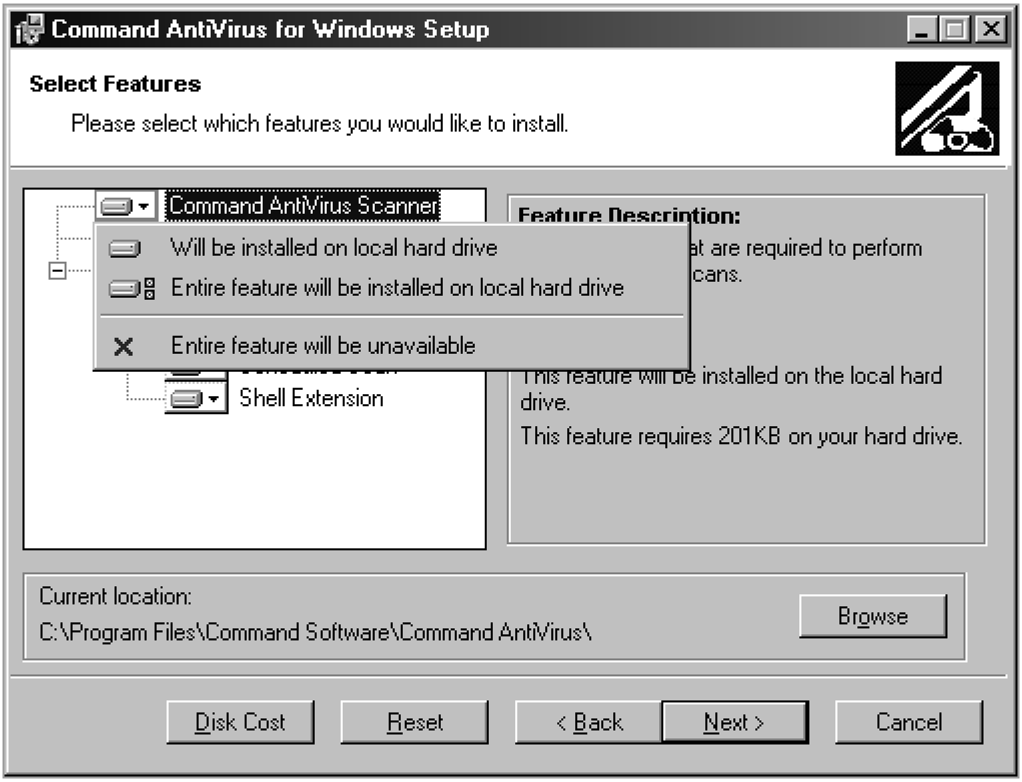
NOTE: For **NetWare Reporting** to work, the Novell® NetWare® client **must** be installed.

  - **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:


Command AntiVirus for Windows Setup
Command AntiVirus Scanner
Shell Extension
Will be installed on local hard drive
Entire feature will be installed on local hard drive
Entire feature will be unavailable
Browse
Disk Cost
Reset
< Back
Next >
Cancel

Select Features

Please select which features you would like to install.

Feature Description:

at are required to perform
cans.

This feature will be installed on the local hard drive.

This feature requires 201KB on your hard drive.

Current location:
C:\Program Files\Command Software\Command AntiVirus\

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**.

10. 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.

    If you selected to install the **Internet Update** feature, go to **Step 12**.

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

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

11. 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.

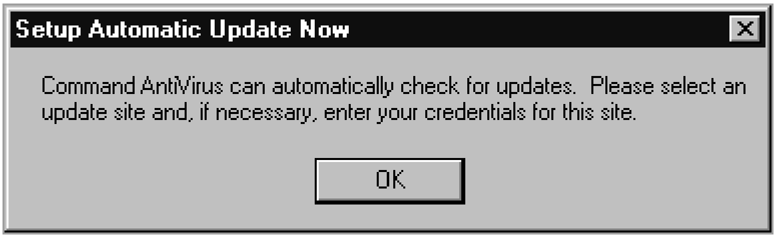
After installing Command AntiVirus, we recommend that you update your virus definition files, and then perform a manual scan of your local drives to ensure that your system is **virus-free**.

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

For information on updating your virus definition files across the network, refer to the ***Network Administration*** chapter of this guide.

12. Please wait while the program copies the Command AntiVirus files to your system. When the copying is complete, the system displays the **Setup Automatic Update Now** dialog box.

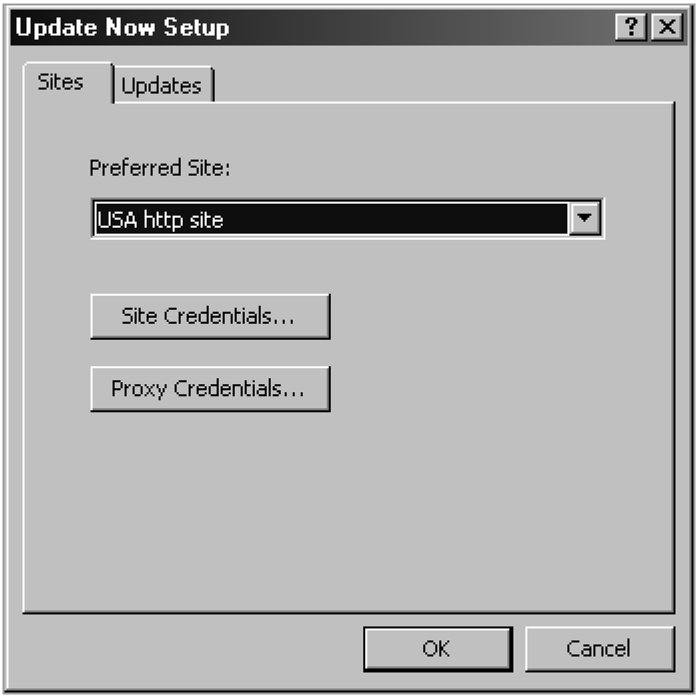
NOTE: If you are reinstalling Command AntiVirus and you kept your customized **Preferences/Update Now** settings, the system displays a dialog box informing you that Command AntiVirus for Windows has been successfully installed. Go to **Step 21**.


Setup Automatic Update Now

Command AntiVirus can automatically check for updates. Please select an update site and, if necessary, enter your credentials for this site.

Setup Automatic Update Now Dialog Box

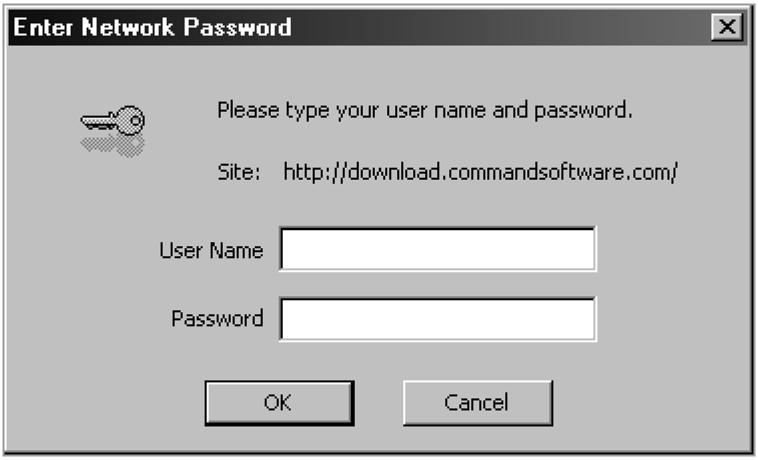
13. Click **OK**. The system displays the **Update Now** dialog box with the **Sites** dialog box in view:



Preferred Site: USA http site

Sites Dialog Box

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


Enter Network Password

Please type your user name and password.

Site: http://download.commandsoftware.com/

User Name

Password

Enter Network Password Dialog Box

16. In the **User Name** text box, type your Command user name.
17. In the **Password** text box, type your Command password.
18. Click **OK**. The system returns to the **Sites** dialog box.
19. 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**.

20. 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.

21. 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.

For information on updating your virus definition files across the network, refer to the ***Network Administration*** 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**.

NT/2K/XP

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.

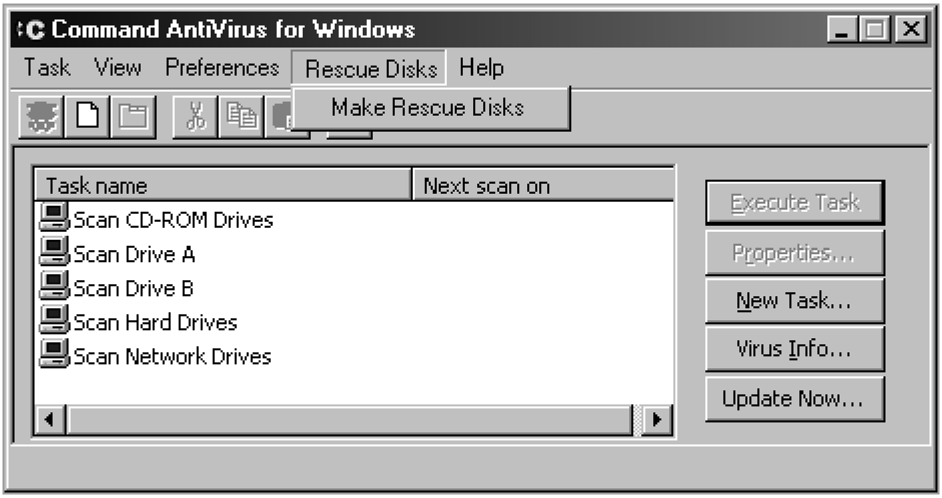
INSTALLATION

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

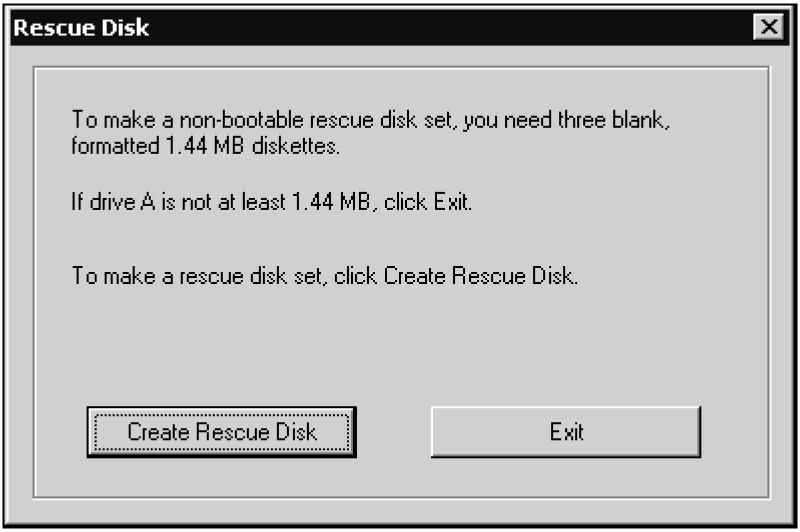
To create a **Rescue Disk** set from the **Rescue Disks** menu, follow these steps:

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

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

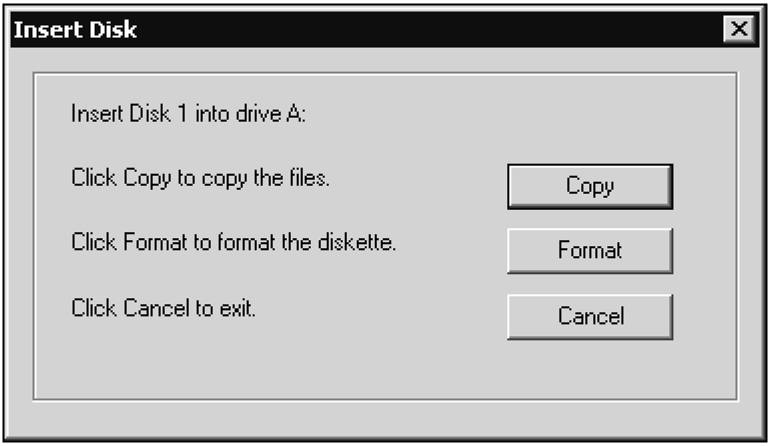
If drive A is not at least 1.44 MB, click Exit.

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

Rescue Disk Dialog Box

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

Insert Disk 1 into drive A:

Click Copy to copy the files.

Click Format to format the diskette.

Click Cancel to exit.

Insert Disk Dialog Box

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.

NT/2K/XP

In Windows NT, Windows 2000, or Windows XP, to perform any of the installation maintenance tasks, <u>**one**</u> of the following conditions <u>**must**</u> be met:

- You are a member of the Administrators group on the local machine
- System policy is set so that you have elevated privileges for installations
- Command AntiVirus has been advertised for the machine.

2K/XP

- Command AntiVirus has been assigned through Group Policy

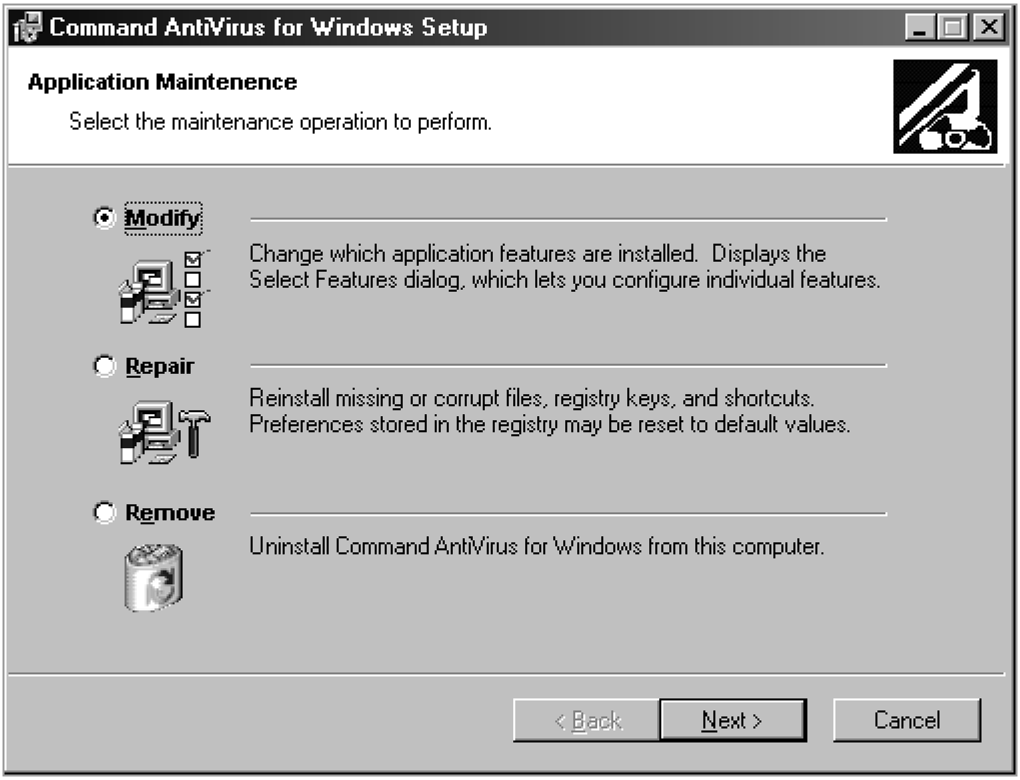
This section contains information on how to:

- 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:



Command AntiVirus for Windows Setup

Application Maintenence

Select the maintenance operation to perform.

● **Modify**

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

○ **Repair**

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

○ **Remove**

Uninstall Command AntiVirus for Windows from this computer.

Application Maintenance Dialog Box

This dialog box contains the following operations:

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

NT/2K/XP

In Windows NT, Windows 2000, or Windows XP, to add or remove features, **one** of the following conditions **must** be met:

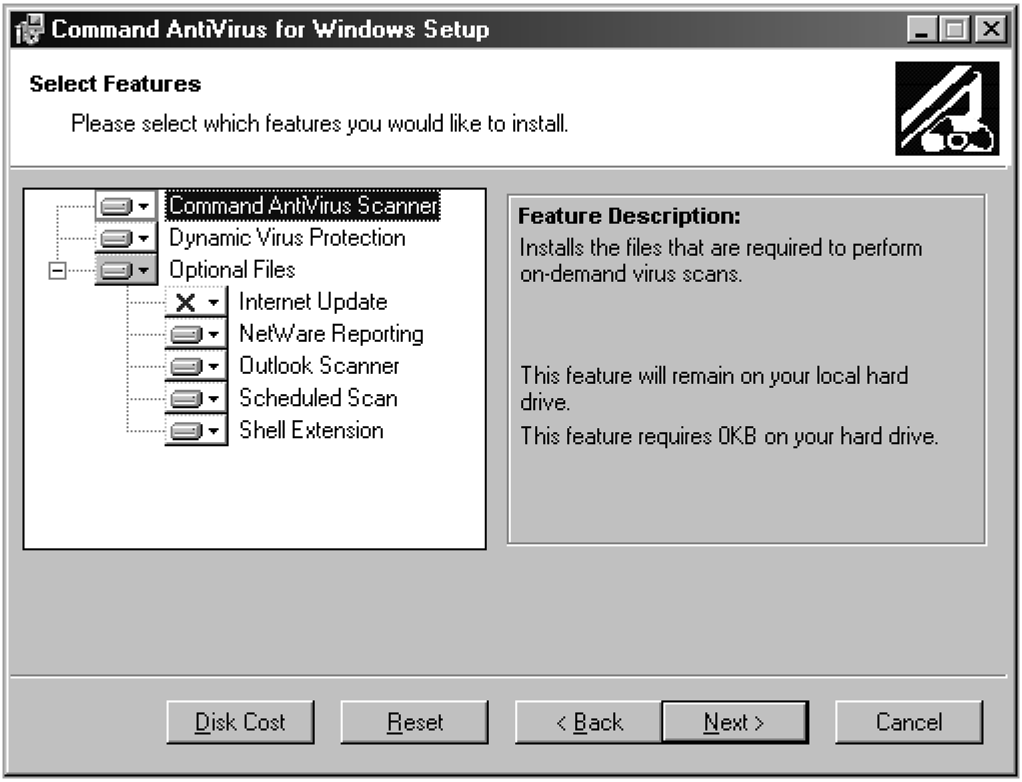
- You are a member of the Administrators group on the local machine
- System policy is set so that you have elevated privileges for installations
- Command AntiVirus has been advertised for the machine.

2K/XP

- Command AntiVirus has been assigned through Group Policy

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:



Command AntiVirus for Windows Setup

Select Features

Please select which features you would like to install.

- Command AntiVirus Scanner
- Dynamic Virus Protection
- Optional Files
  - ☒ Internet Update
  - NetWare Reporting
  - Outlook Scanner
  - Scheduled Scan
  - Shell Extension

Feature Description:

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

This feature will remain on your local hard drive.

This feature requires 0KB on your hard drive.

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**.

7. 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.

8. 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 Command AntiVirus, **one** of the following conditions **must** be met:

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

To repair the Command AntiVirus installation, 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 **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.

NT/2K/XP

In Windows NT, Windows 2000, or Windows XP, to remove Command AntiVirus, **one** of the following conditions **must** be met:

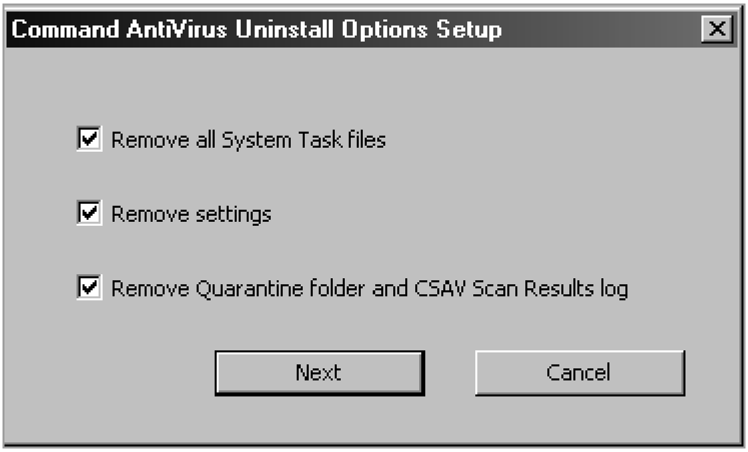
- You are a member of the Administrators group on the local machine
- System policy is set so that you have elevated privileges for installations
- Command AntiVirus has been advertised for the machine.

2K/XP

- Command AntiVirus has been assigned through Group Policy

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:



Command AntiVirus Uninstall Options Setup

☑ Remove all System Task files

☑ Remove settings

☑ Remove Quarantine folder and CSAV Scan Results log

CSAV Unistall 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:

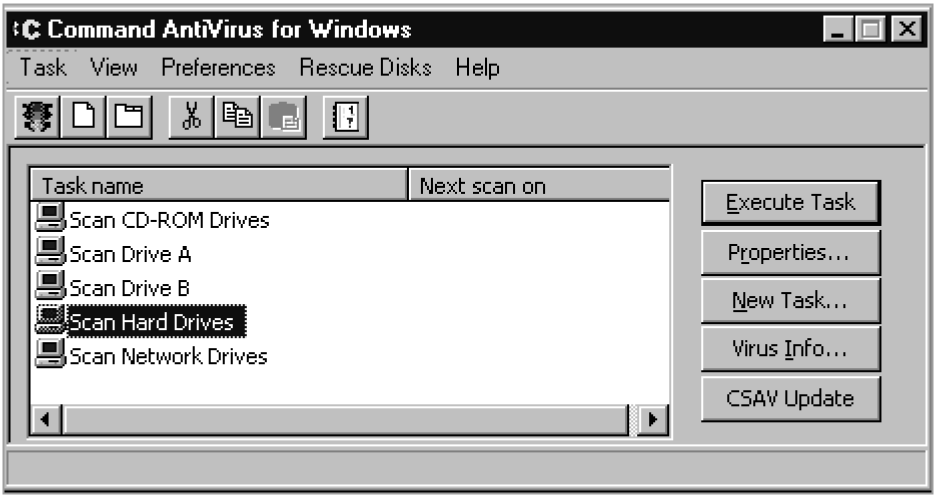
- Become familiar with the **Command AntiVirus Main** dialog box
- Create and use a recovery Rescue Disk Set
- Start or schedule an on-demand scan
- Understand what happens when a virus infection is found through on-access scanning
- View scan results
- Customize how and where scan results are reported
- 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:



Task name	Next scan on
Scan CD-ROM Drives	
Scan Drive A	
Scan Drive B	
Scan Hard Drives	
Scan Network Drives	

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:

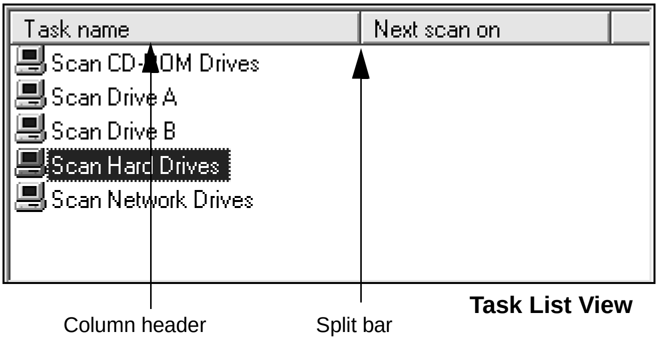
- Task Window
- Command Buttons
- Shortcut Menu
- Menu Bar
- Toolbar Buttons
- CSAV Icon
- Command AntiVirus Shortcut Menu

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

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**.

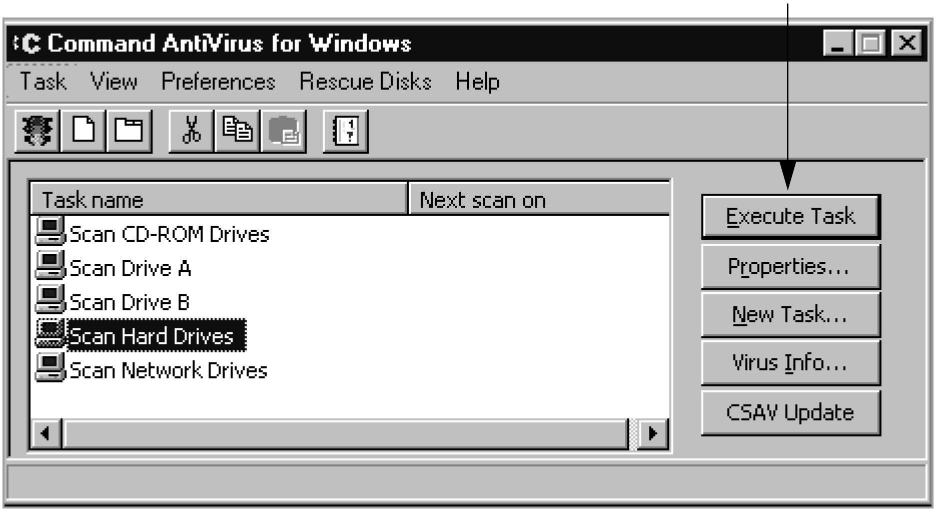
Sizing the Columns

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 buttons



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**.

CSAV Update Button

This button allows a user on the network to start the program that checks for updates (**CUAGENT.EXE**) on demand. By default, this program starts when a user logs on to the machine. The program then carries out an Enterprise update of Command AntiVirus virus definition files and components from an administrative image. The **CSAV Update** button is installed by default. For more information, refer to **Updating Command AntiVirus** located later in this chapter.

Update Now Button

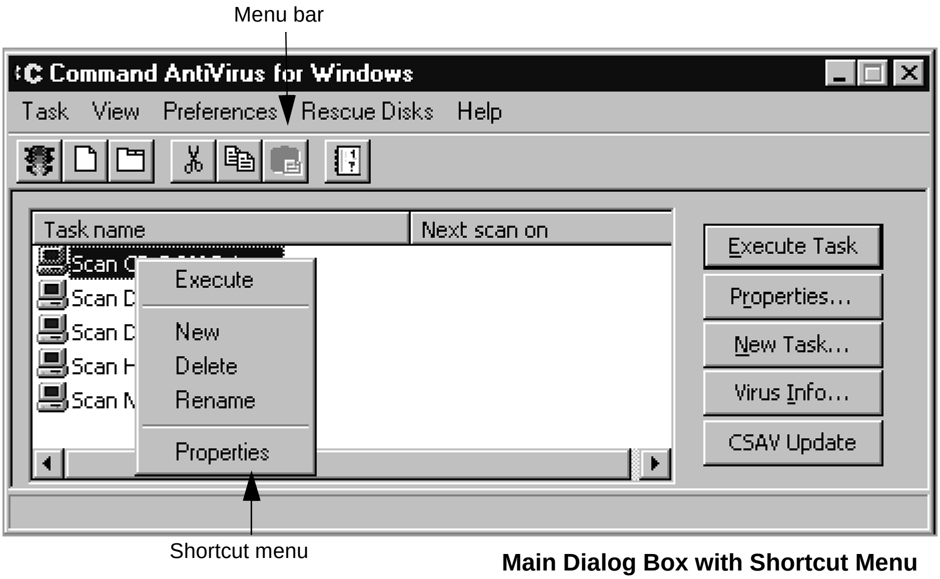
This button is available **only** if you install the **Internet Update** feature that replaces the **CSAV Update** button.

The **Update Now** button allows the end-user to update the Command AntiVirus virus definition files, components, and full product on-demand through the Internet. 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

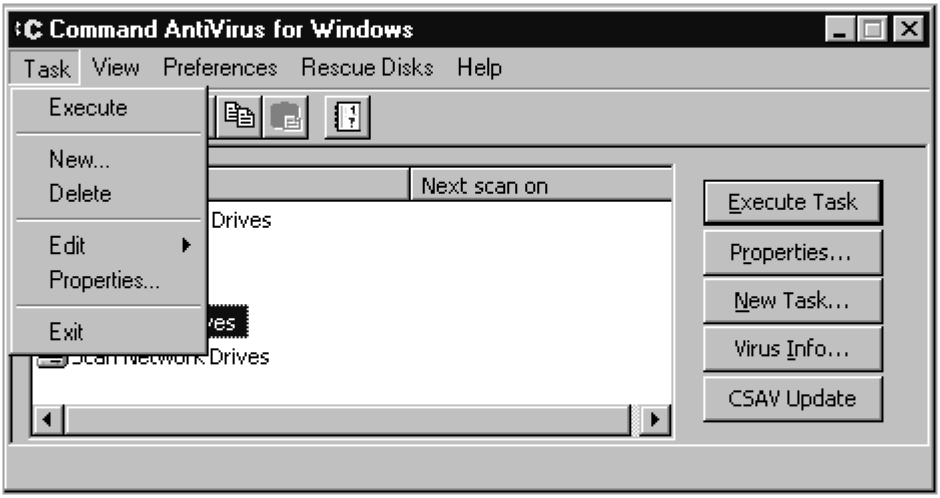
MENU BAR

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:



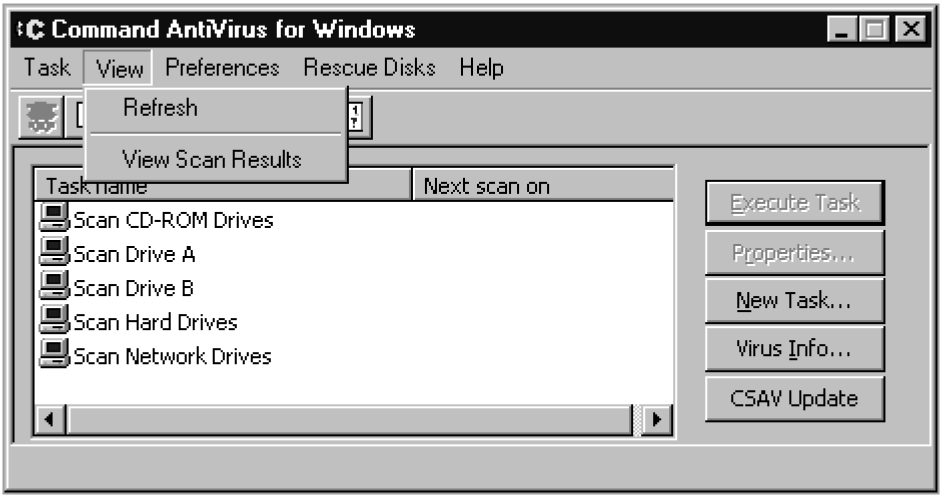
Main Dialog Box with Task Menu

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.

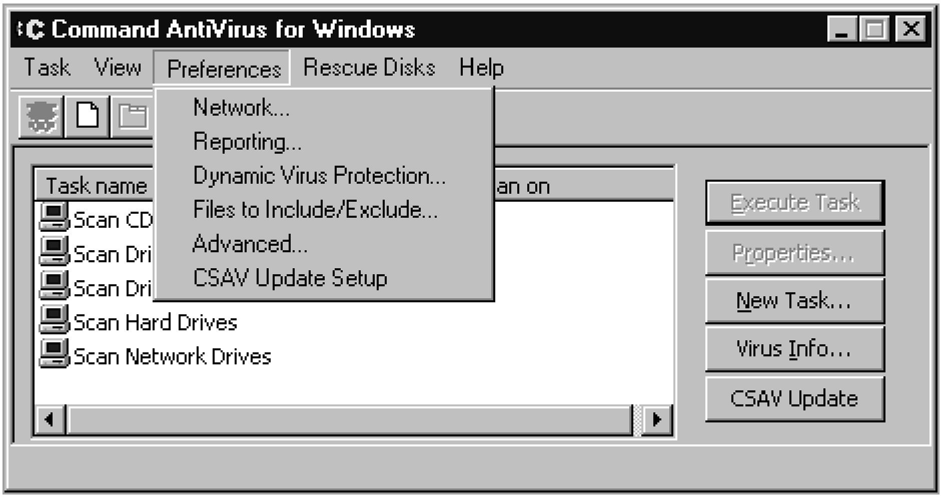
For more information on updating the Task Window, refer to **Updating the Task Window Information** located previously in this chapter.

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.

Administrator’s 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.

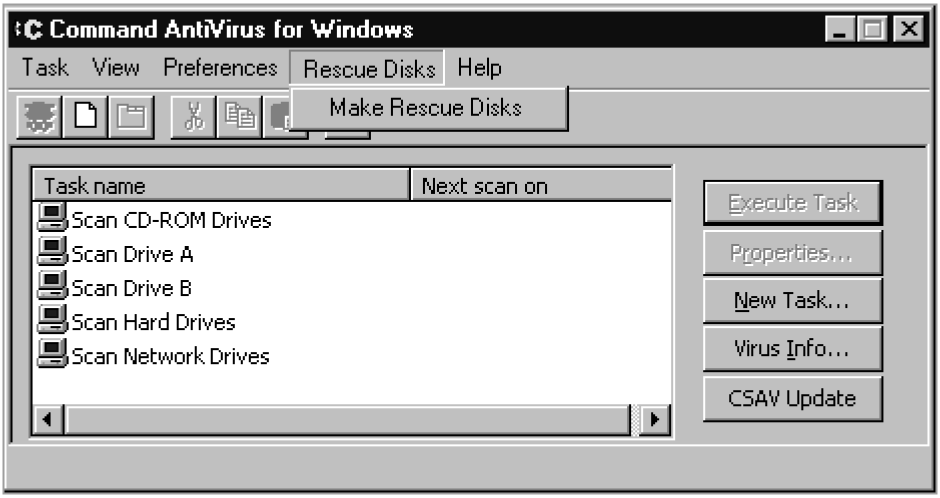
- **CSAV Update Setup** – Schedule the activation of updating the administrative image on a server. For more information, refer to **Updating Command AntiVirus** located later in this chapter.

NOTE: The **CSAV Update Setup** menu item is available **<u>only</u>** if you have the Windows® Task Scheduler installed.

Administrators can customize these features by using the Custom Installation Wizard for Command Antivirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this guide.

Rescue Disks Menu

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



Task name	Next scan on
Scan CD-ROM Drives	
Scan Drive A	
Scan Drive B	
Scan Hard Drives	
Scan Network Drives	

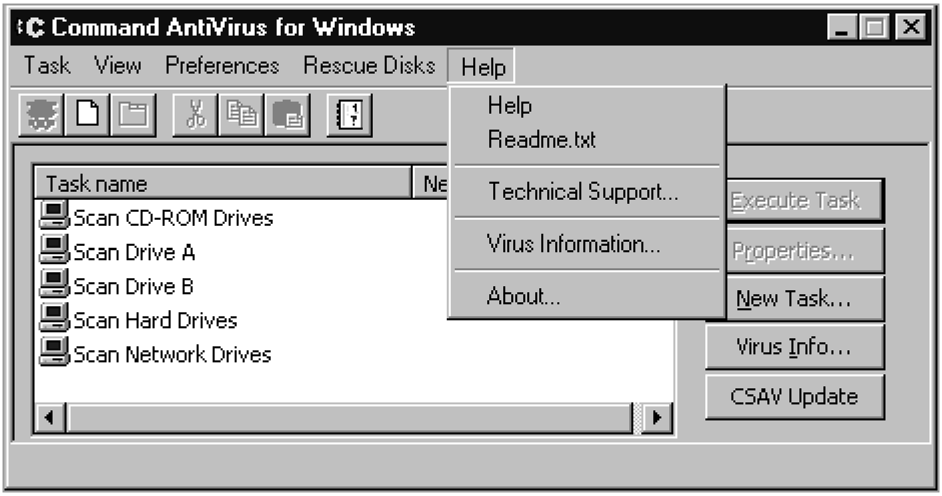
Main Dialog Box with Rescue Disks Menu

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.

Administrators can customize CSAV to hide this menu by using the Custom Installation Wizard for Command Antivirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this administrator's guide.

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:

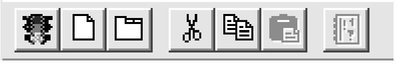
- **Help –** Find information on a specific topic
- **Readme.txt** – View the Readme.txt file

- **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.

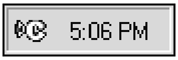


NOTE: To see a ToolTip that identifies the function of a particular button, move the mouse pointer over any toolbar button.

OTHER WAYS TO ACCESS COMMAND ANTIVIRUS

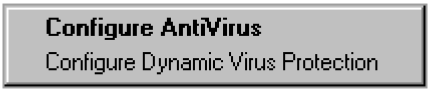
You can open the **Command AntiVirus Main** dialog box in several ways:

- 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.

Administrators can customize Command AntiVirus to hide the yellow C icon by using the Custom Installation Wizard for Command Antivirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this administrator's guide.

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.

Administrators can customize CSAV to hide this menu by using the Custom Installation Wizard for Command Antivirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this administrator's guide.

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.

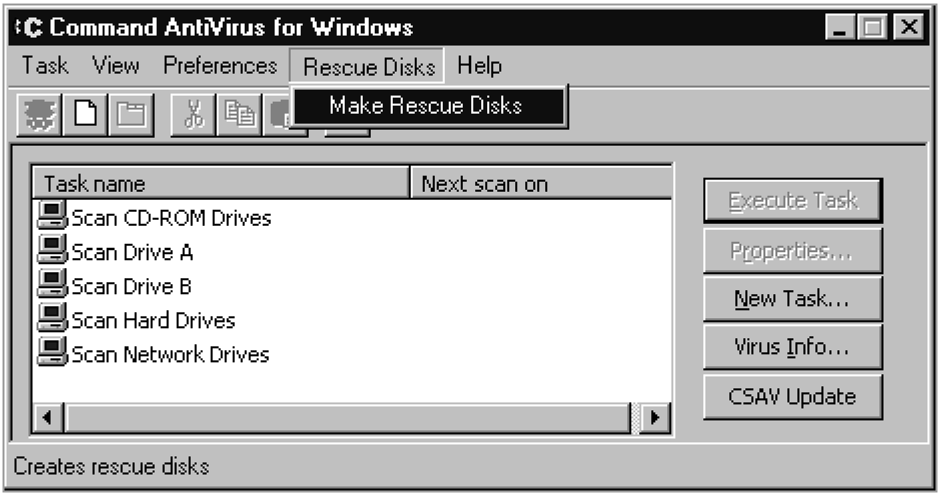
You can use **Rescue Disk 1** on NTFS systems at any time to repair damaged or infected boot sector information.

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

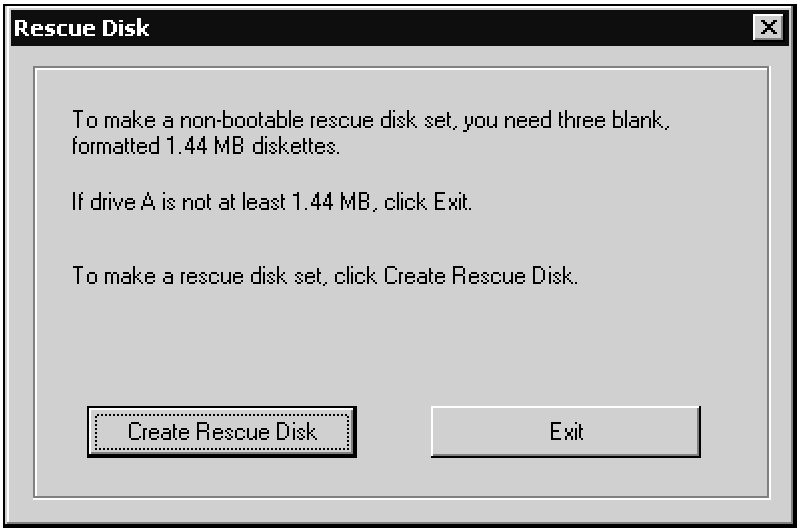
To create a **Rescue Disk** set from the **Rescue Disks** menu, follow these steps:

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

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

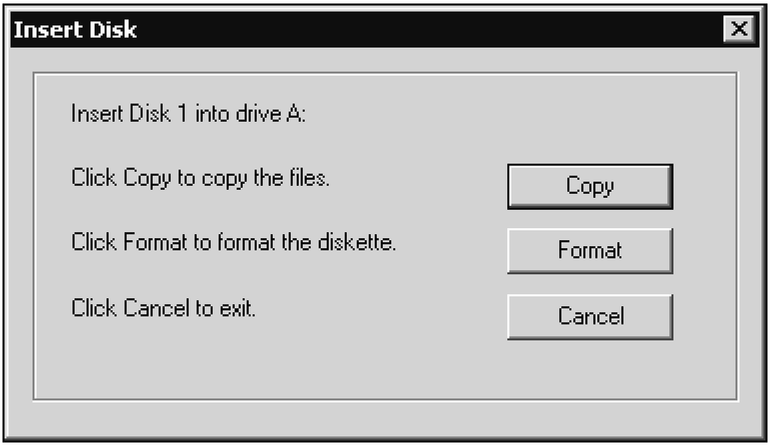
If drive A is not at least 1.44 MB, click Exit.

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

Rescue Disk Dialog Box

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

Insert Disk 1 into drive A:

Click Copy to copy the files.

Click Format to format the diskette.

Click Cancel to exit.

Insert Disk Dialog Box

4. Insert **Disk 1** into drive A, and click **Copy**. The system 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.

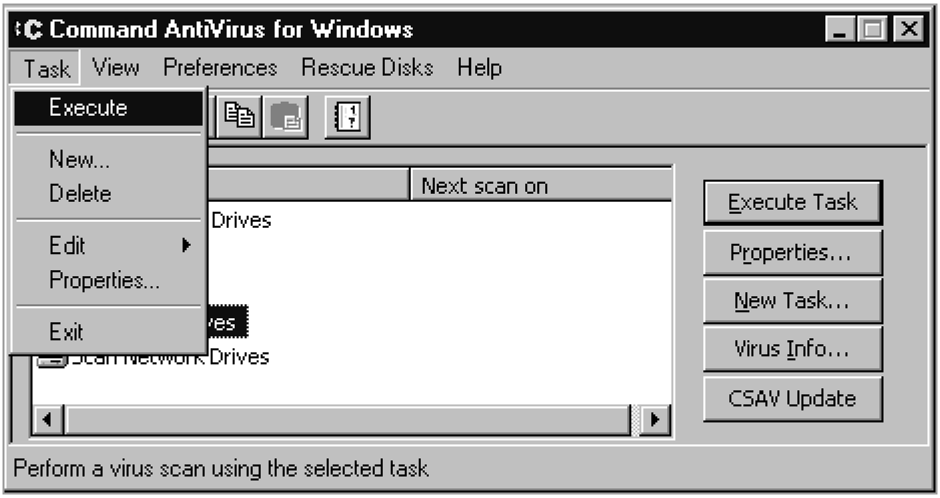
You can also create a new scan task through the **Task** menu. For more information, refer to **Creating A New Scan Task** located later in this chapter.

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:

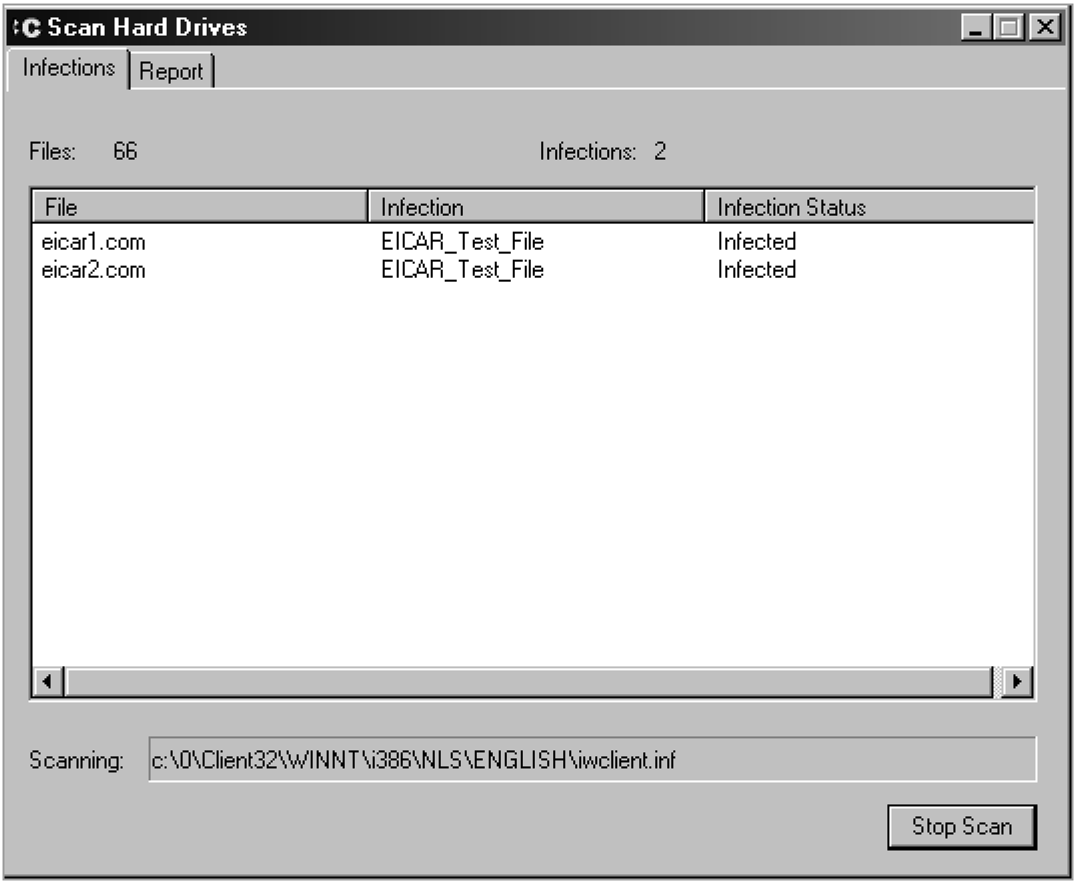


Perform a virus scan using the selected task

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.



Files: 66

Infections: 2

File	Infection	Infection Status
eicar1.com	EICAR_Test_File	Infected
eicar2.com	EICAR_Test_File	Infected

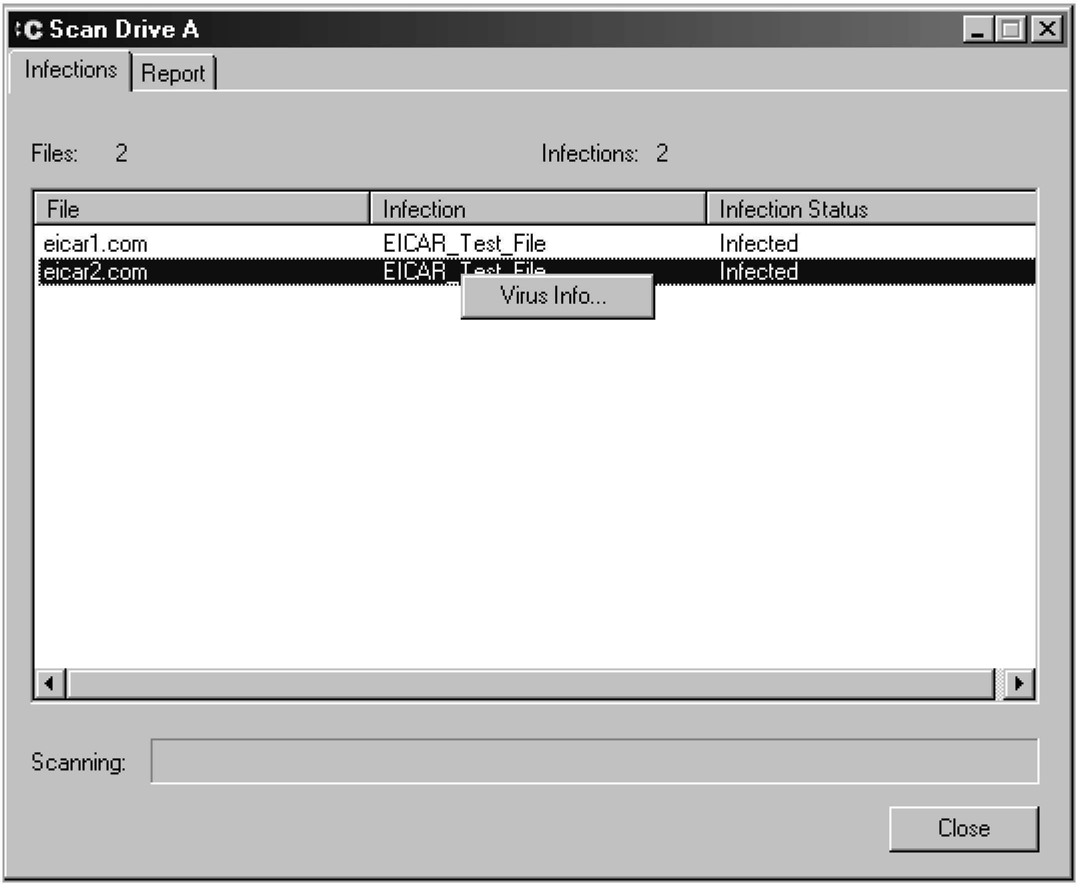
Scanning: c:\0\Client32\WINNT\i386\NLS\ENGLISH\iwclient.inf

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:



Files: 2 Infections: 2

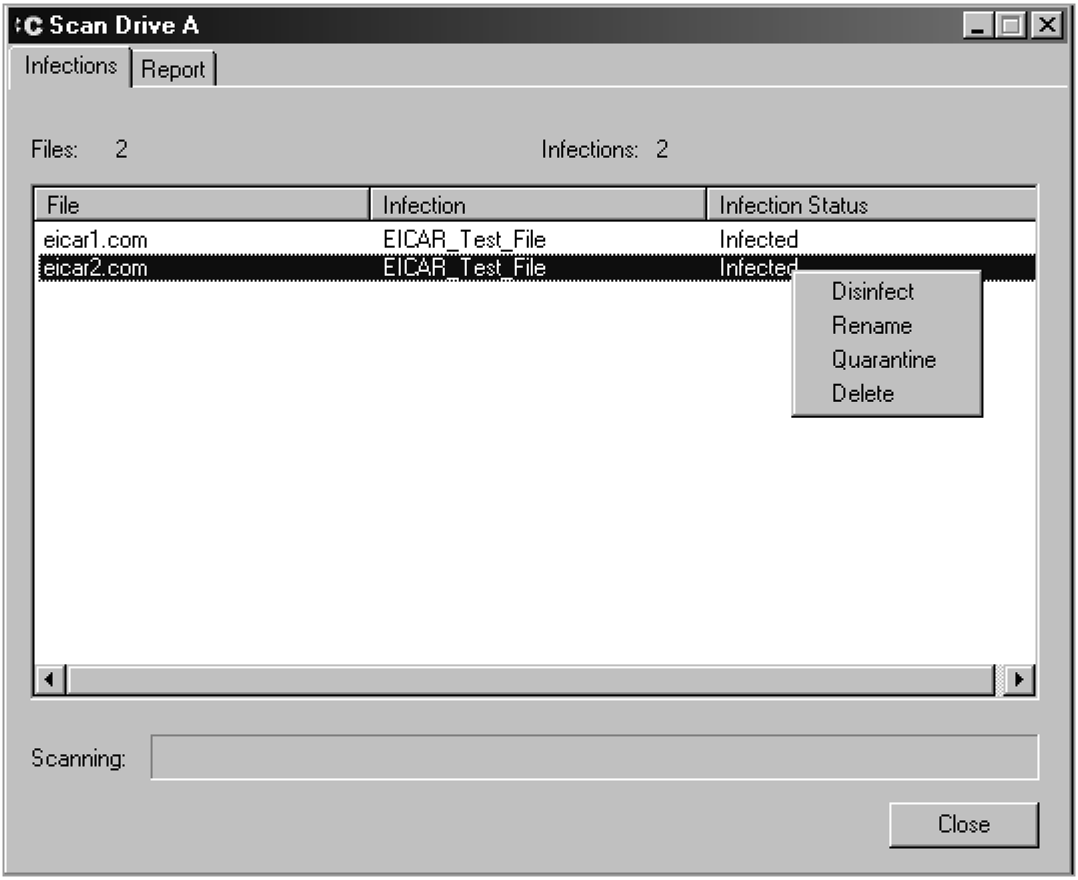
File	Infection	Infection Status
eicar1.com	EICAR_Test_File	Infected
eicar2.com	EICAR_Test_File	Infected

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:



Files: 2 Infections: 2

File	Infection	Infection Status
eicar1.com	EICAR_Test_File	Infected
eicar2.com	EICAR_Test_File	Infected

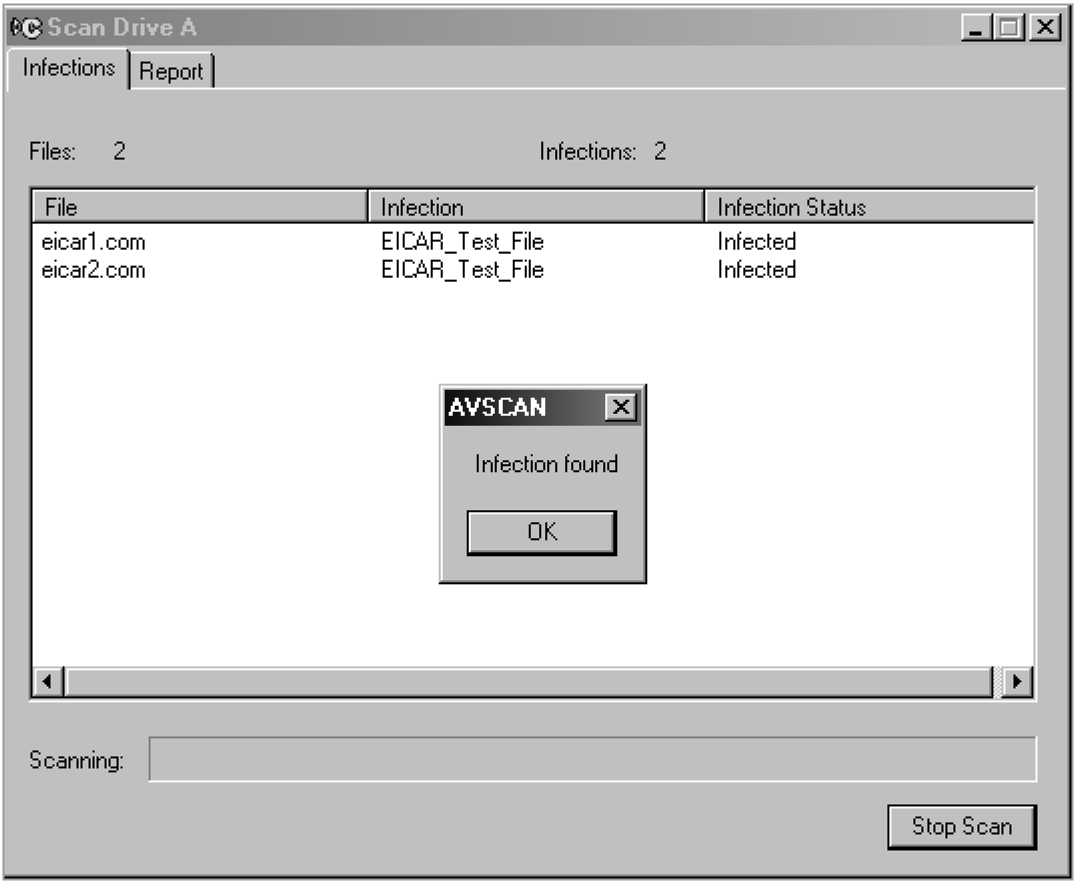
Infections Dialog Box – Action On Infection

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:



Files: 2 Infections: 2

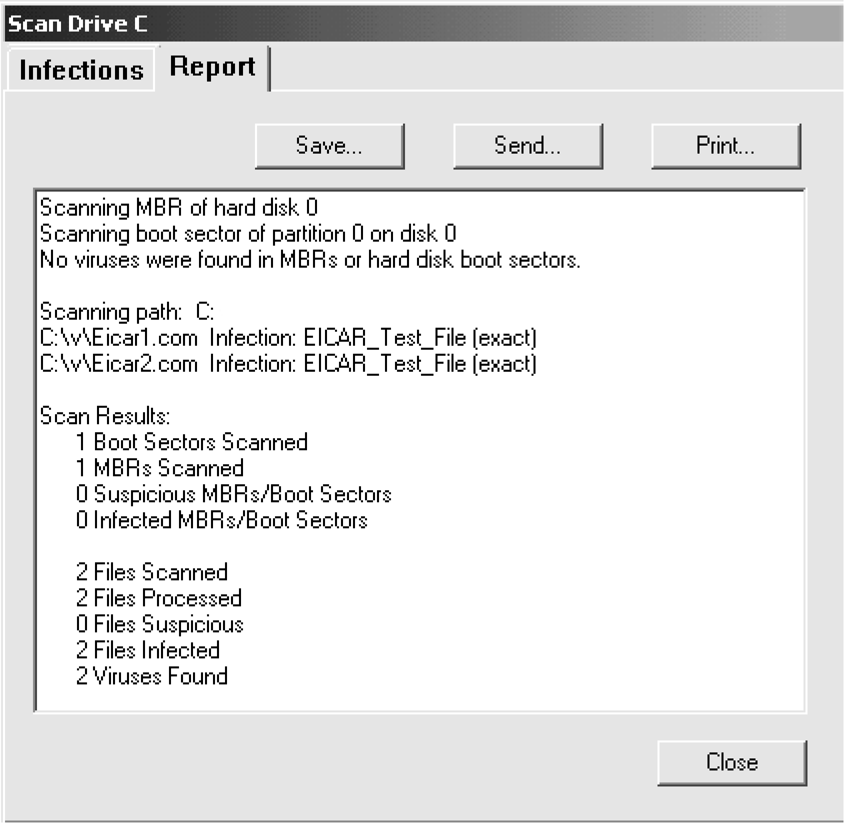
File	Infection	Infection Status
eicar1.com	EICAR_Test_File	Infected
eicar2.com	EICAR_Test_File	Infected

Infection found

Scanning:

AVScan Message Box

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



```
Scanning MBR of hard disk 0
Scanning boot sector of partition 0 on disk 0
No viruses were found in MBRs or hard disk boot sectors.

Scanning path:  C:
C:\v\Eicar1.com  Infection: EICAR_Test_File (exact)
C:\v\Eicar2.com  Infection: EICAR_Test_File (exact)

Scan Results:
    1 Boot Sectors Scanned
    1 MBRs Scanned
    0 Suspicious MBRs/Boot Sectors
    0 Infected MBRs/Boot Sectors

    2 Files Scanned
    2 Files Processed
    0 Files Suspicious
    2 Files Infected
    2 Viruses Found
```

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.

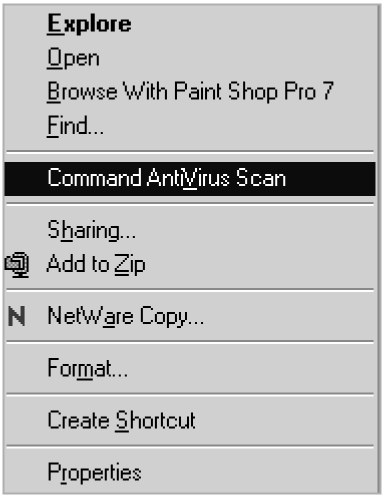
NOTE: You can also start an on-demand scan by selecting a **Task name** and clicking the **Execute Task** button in the **Command AntiVirus Main** dialog box or the **Execute** button on the toolbar.

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.

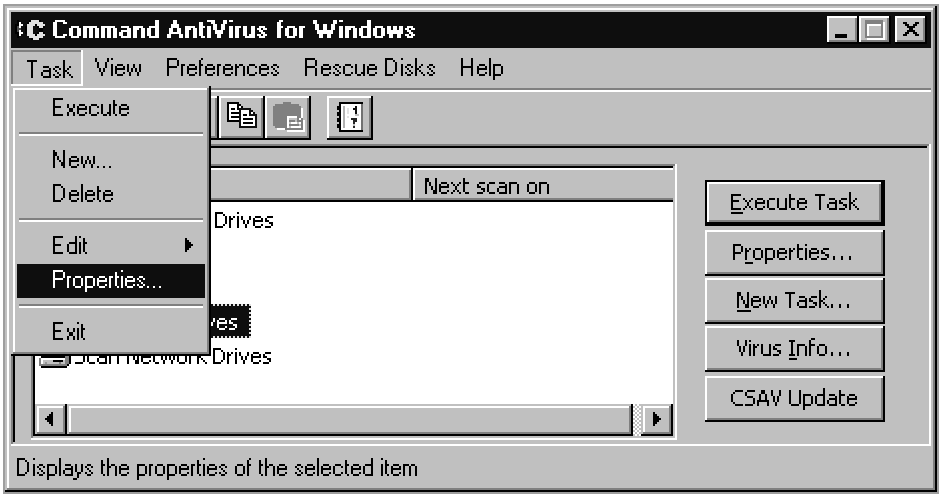
In Windows NT, Windows 2000, or Windows XP, you can also view scan results in the Windows Event Viewer if you selected the **Report to Application Log** option.

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:

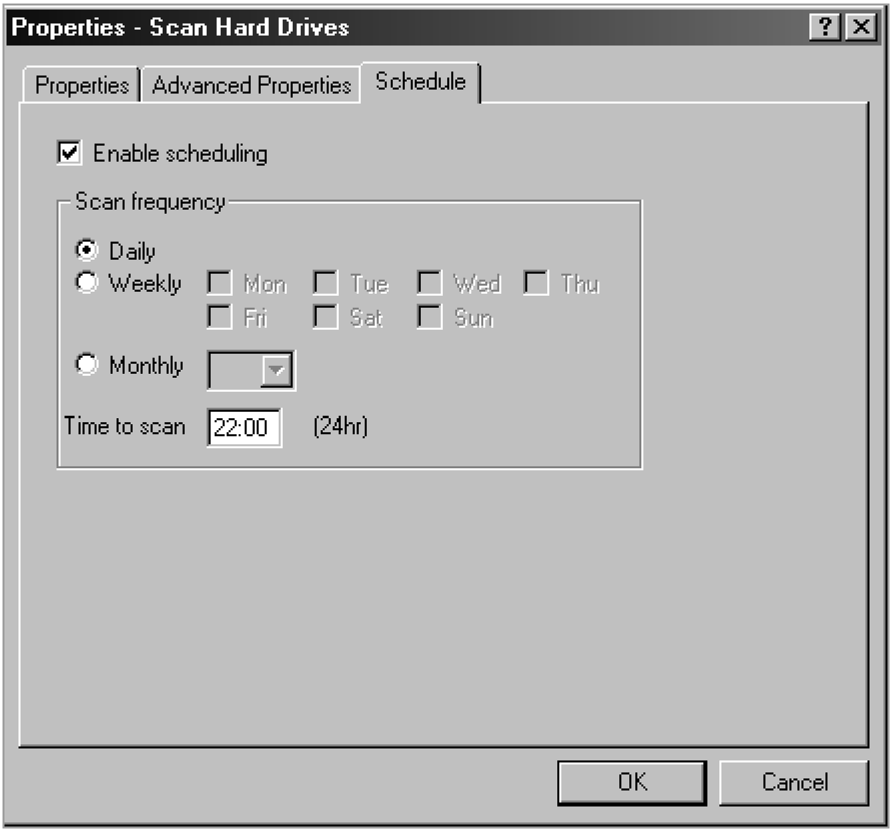


Task Menu

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:



☑ Enable scheduling

Scan frequency

● Daily

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

○ Monthly

Time to scan 22:00 (24hr)

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.

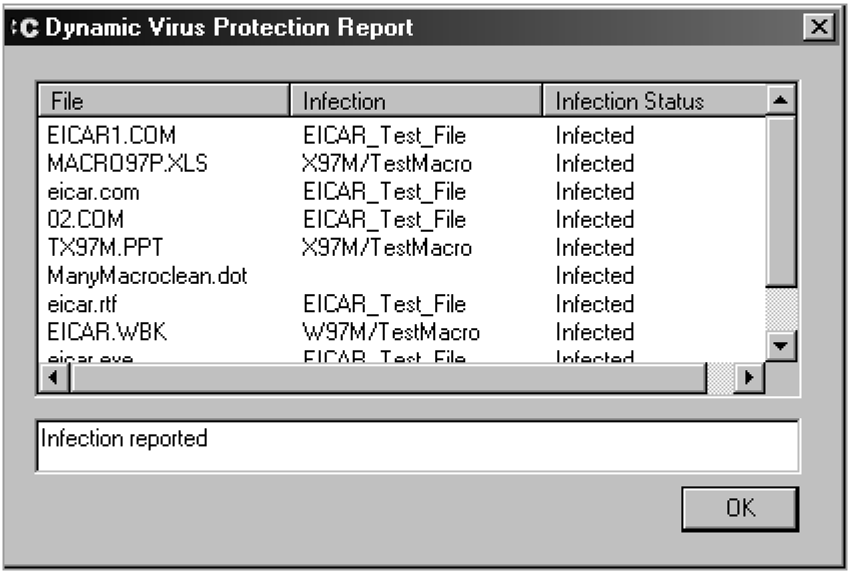
8. Click OK.

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 Repor**t log. It also provides information on how to view the information in the log, clear the log, and exit the log.



Dynamic Virus Protection Report

File	Infection	Infection Status
EICAR1.COM	EICAR_Test_File	Infected
MACRO97P.XLS	X97M/TestMacro	Infected
eicar.com	EICAR_Test_File	Infected
02.COM	EICAR_Test_File	Infected
TX97M.PPT	X97M/TestMacro	Infected
ManyMacroclean.dot		Infected
eicar.rtf	EICAR_Test_File	Infected
EICAR.WBK	W97M/TestMacro	Infected
eicar.exe	EICAR_Test_File	Infected

Infection reported

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.

USING COMMAND ANTIVIRUS

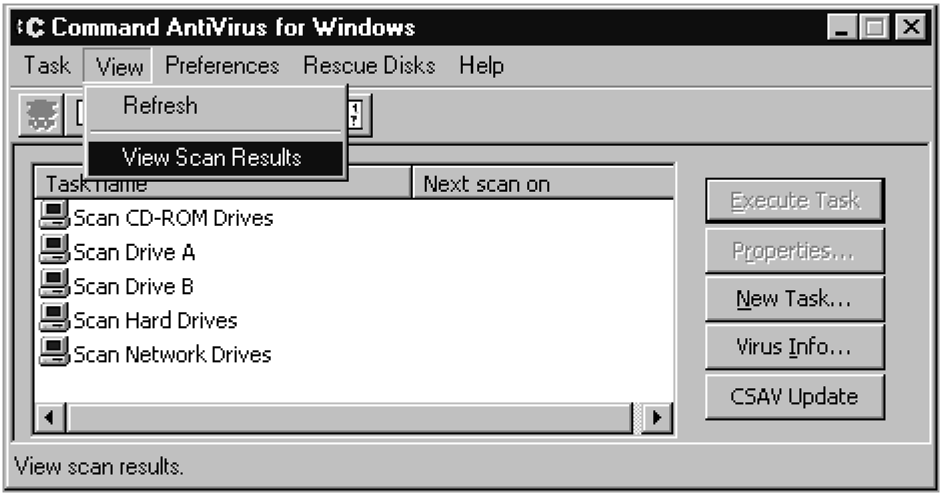
FROM THE VIEW MENU

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:

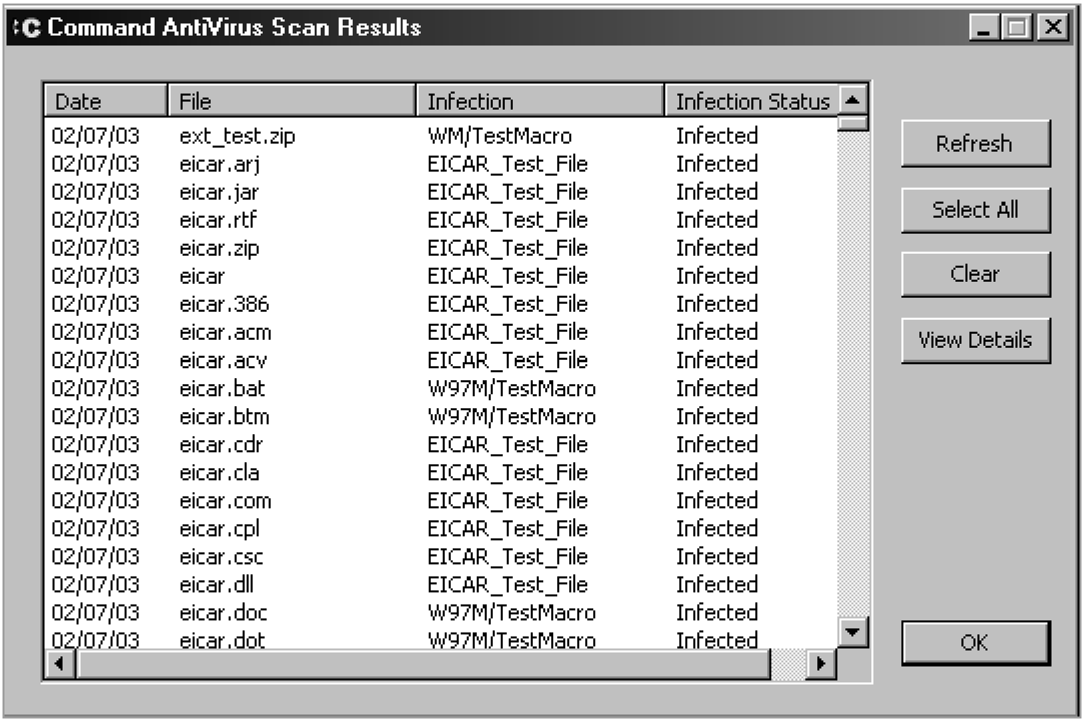


Task name	Next scan on
Scan CD-ROM Drives	
Scan Drive A	
Scan Drive B	
Scan Hard Drives	
Scan Network Drives	

View scan results.

View Menu

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



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**.

USING COMMAND ANTIVIRUS

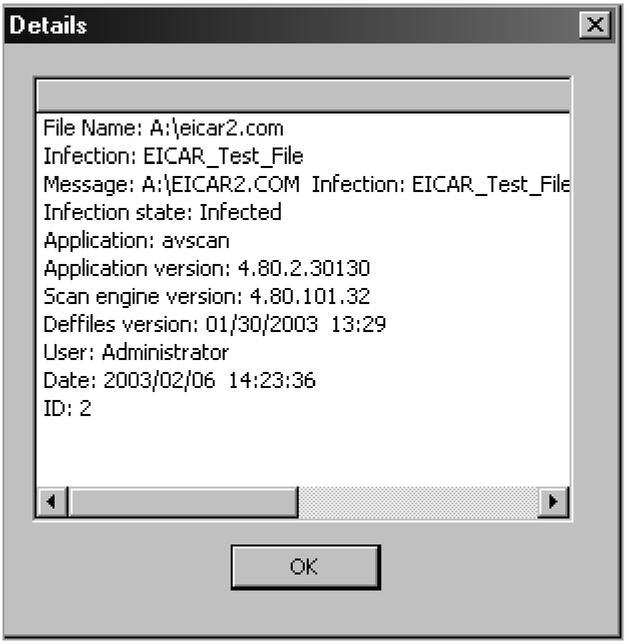
- **Infection** – Identifies the type of virus infection found.
- **Infection Status** – Identifies the present state of the virus infection, for example, **Infected**.

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.



```
File Name: A:\eicar2.com
Infection: EICAR_Test_File
Message: A:\EICAR2.COM  Infection: EICAR_Test_File
Infection state: Infected
Application: avscan
Application version: 4.80.2.30130
Scan engine version: 4.80.101.32
Deffiles version: 01/30/2003  13:29
User: Administrator
Date: 2003/02/06  14:23:36
ID: 2
```

Details Dialog Box

Adding the Latest Scan Results

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

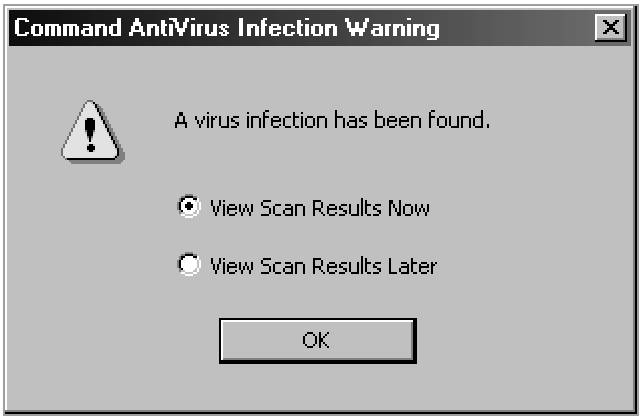
Clearing the Scan Results

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:



Command AntiVirus Infection Warning

A virus infection has been found.

● View Scan Results Now

○ View Scan Results Later

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**.

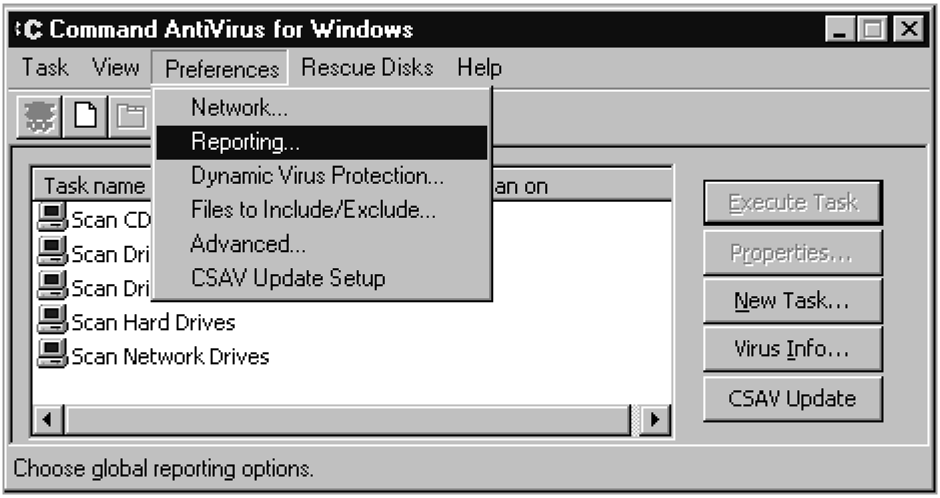
In Windows NT, Windows 2000, and Windows XP, to change **Preferences**, you **must** be signed on as a member of the Administrators group on the local machine. If you are not, all of the menu items except **Advanced** are available **only** for viewing.

Administrators can enable this option by using the Custom Installation Wizard for Command AntiVirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this administrator’s guide.

Logging Scan Results

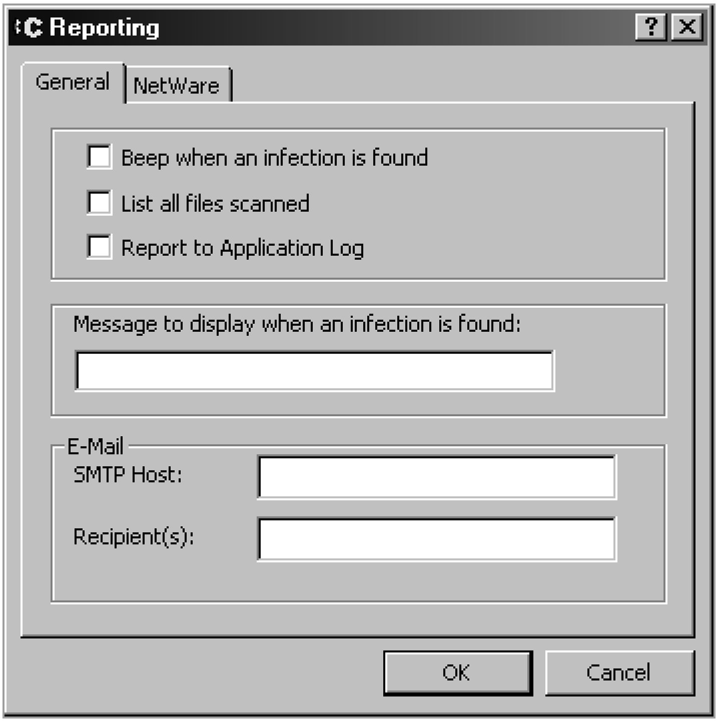
To log each occurrence of a virus found in the **Event Viewer Application Log**, follow these steps:

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:



☐ Beep when an infection is found

☐ List all files scanned

☐ Report to Application Log

Message to display when an infection is found:

E-Mail

SMTP Host:

Recipient(s):

General Dialog Box

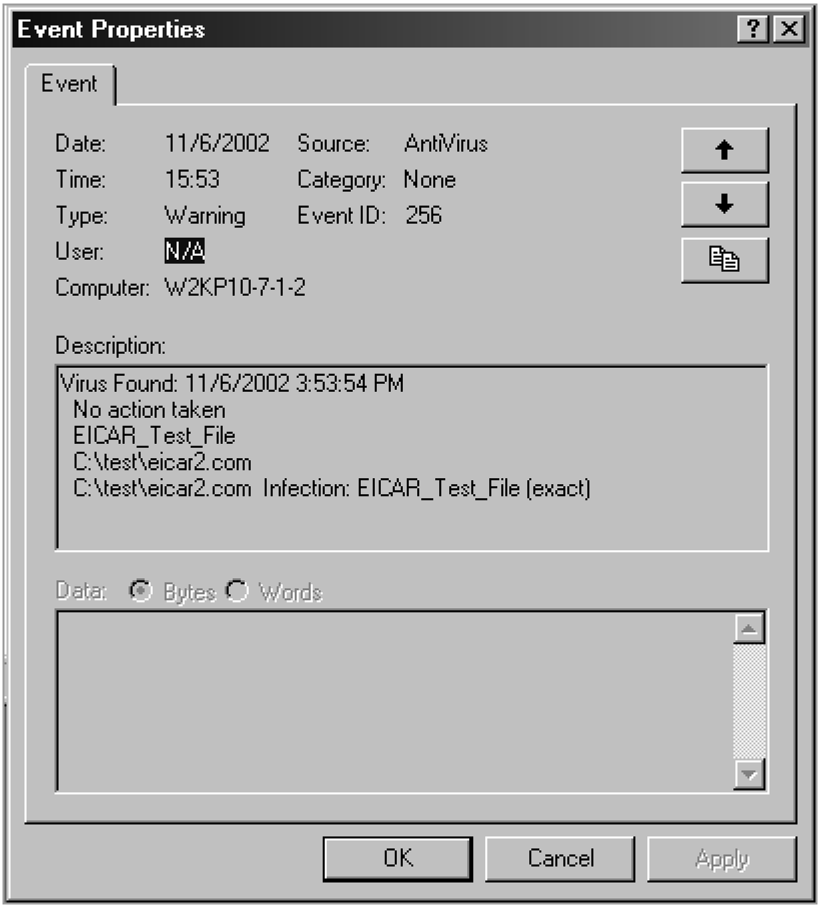
3. Select the **Report to Application Log** check box.
4. Click **OK**.

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:



Date: 11/6/2002
Time: 15:53
Type: Warning
User: N/A
Computer: W2KP10-7-1-2
Source: AntiVirus
Category: None
Event ID: 256

Description:

```
Virus Found: 11/6/2002 3:53:54 PM
  No action taken
  EICAR_Test_File
  C:\test\eicar2.com
  C:\test\eicar2.com  Infection: EICAR_Test_File (exact)
```

Data: ● Bytes ○ Words

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.

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.

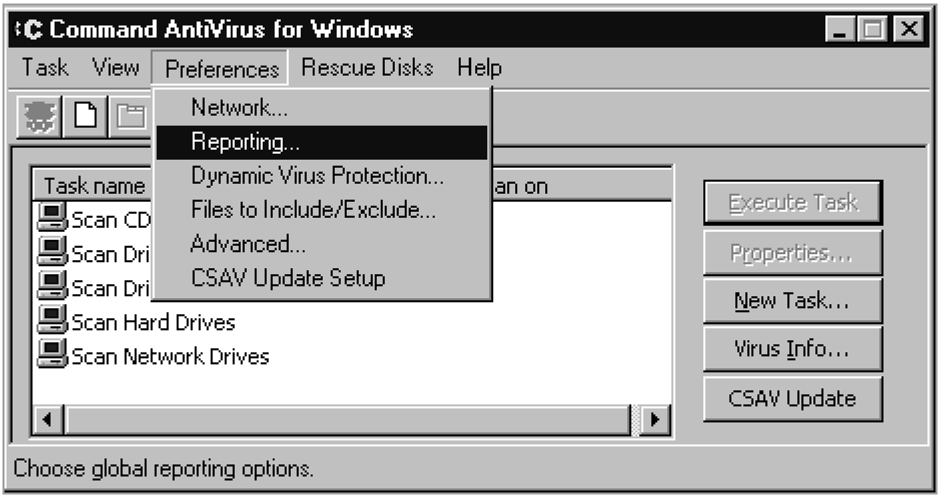
This section contains information on how to set these scan reporting options.

Administrator's 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.

Administrators can enable this option by using the Custom Installation Wizard for Command AntiVirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this administrator's guide.

To set the reporting options, follow these steps:

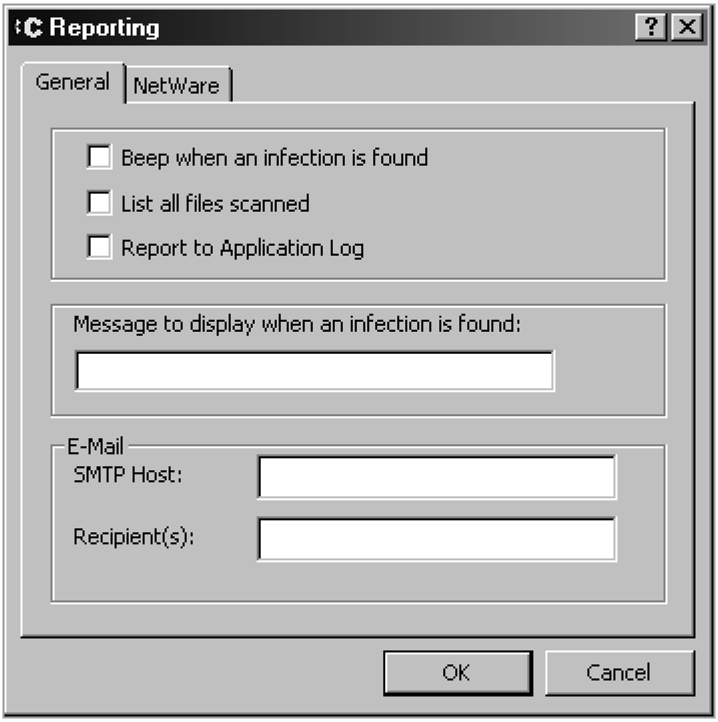
1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Choose global reporting options.

Preferences Menu

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



□ Beep when an infection is found

□ List all files scanned

□ Report to Application Log

Message to display when an infection is found:

E-Mail

SMTP Host:

Recipient(s):

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.

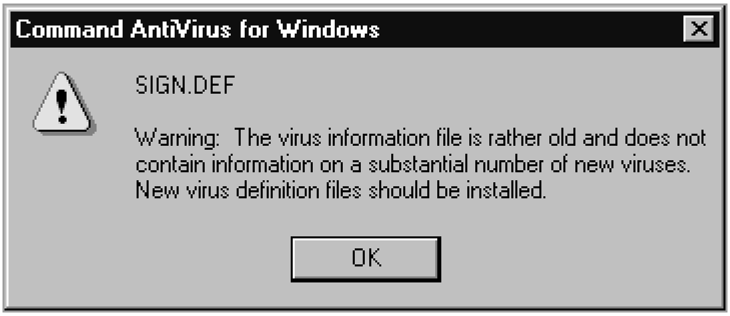
5. Click **OK**.

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:



SIGN.DEF

Warning: The virus information file is rather old and does not contain information on a substantial number of new viruses. New virus definition files should be installed.

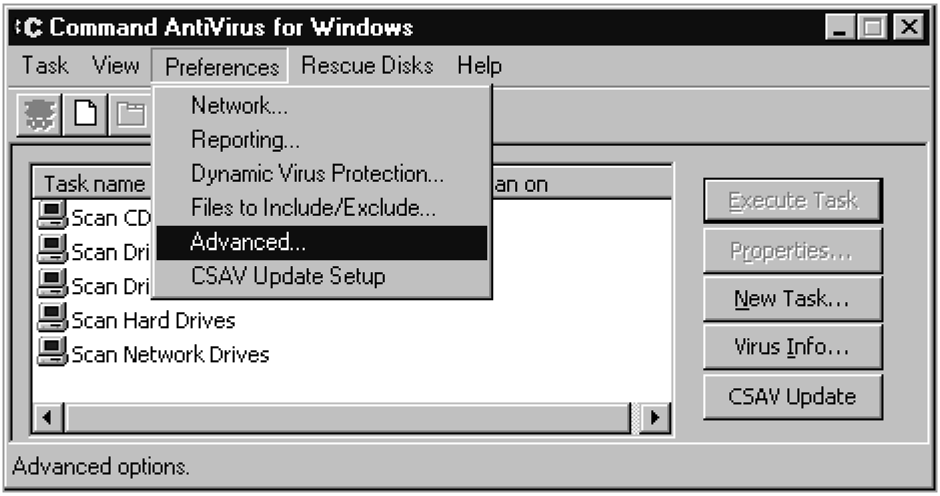
Virus Definition Files Warning Message

Administrators can enable this option by using the Custom Installation Wizard for Command AntiVirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this administrator’s guide.

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

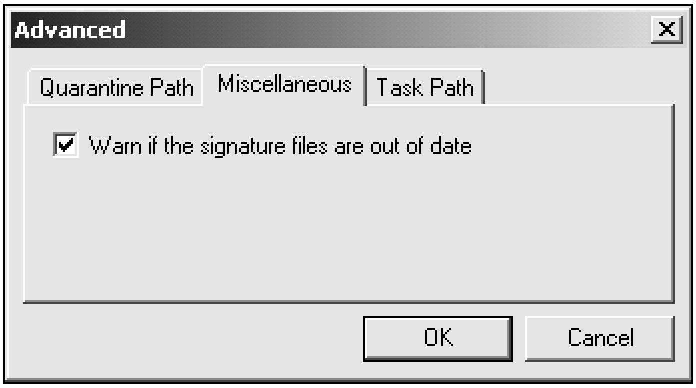
To receive a warning when the virus definition files are out-of-date, follow these steps:

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:



☑ Warn if the signature files are out of date

Miscellaneous Dialog Box

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

UPDATING COMMAND ANTIVIRUS

To ensure that your computer remains virus-free, it is important that your Command AntiVirus software is kept up-to-date.

Command AntiVirus for Windows Enterprise allows you to choose **one** of two methods of updating. The default method is the **Enterprise Update** in which workstations update from an administrative image. The second method is the **Internet Update** in which users update directly from the Internet.

In the **Enterprise Update**, the **CSAV Update** button in the **Command AntiVirus Main** dialog box allows users to activate the updating process on-demand. The **Preferences**/**CSAV Update Setup** menu item, allows administrators to schedule the activation of updating from the administrative image.

NOTE: The **CSAV Update Setup** menu item is available **only** if you have the Windows® Task Scheduler installed.

In the **Internet Update**, users 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, they can set the **Update Now** feature to check for updates automatically.

NOTE: The **Internet Update** feature is **not** installed by default. You must install this feature during installation. For more information, refer to the ***Installation*** chapter of this guide.

NT/2K/XP

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.

This section contains information on both the **Enterprise Update** feature and the **Internet Update** feature.

ENTERPRISE UPDATE FEATURE

As part of COMMANDCentral, administrators in an Enterprise environment can use the Command AntiVirus Download Manager to schedule automatic downloads of virus definition files, component updates, and full product upgrades. The Download Manager also allows administrators to apply these updates and upgrades to administrative images automatically. For more information on the Download Manager, refer to **Command AntiVirus Download Manager** located in the ***COMMANDCentral*** chapter of this guide.

Command AntiVirus for Windows Enterprise contains an agent (**CUAGENT.EXE**) that detects changes to the administrative image. By default, this program is started when a user logs onto the machine. In the **Enterprise Update**, the **CSAV Update** button in the **Command AntiVirus Main** dialog box allows a user on the network to start the program on demand from within the GUI. The program then carries out an Enterprise update of Command AntiVirus virus definition files and components from an administrative image.

In the **Enterprise Update**, the **Preferences**/**CSAV Update Setup** menu item, allows administrators to schedule **CUAGENT.EXE** to run at a particular time on a server. The program then carries out an update from the administrative image.

The **Enterprise Update feature** is installed by default. For an alternate method of updating, refer to **Internet Update Feature** located later in this section.

This section contains information on how to use the **CSAV Update** button, and how to schedule **CUAGENT.EXE** to run on an SPD.

Using the CSAV Update Button

NT/2K/XP

In Windows NT, Windows 2000, or Windows XP, to use the **CSAV Update** button, **<u>one</u>** of the following conditions **<u>must</u>** be met:

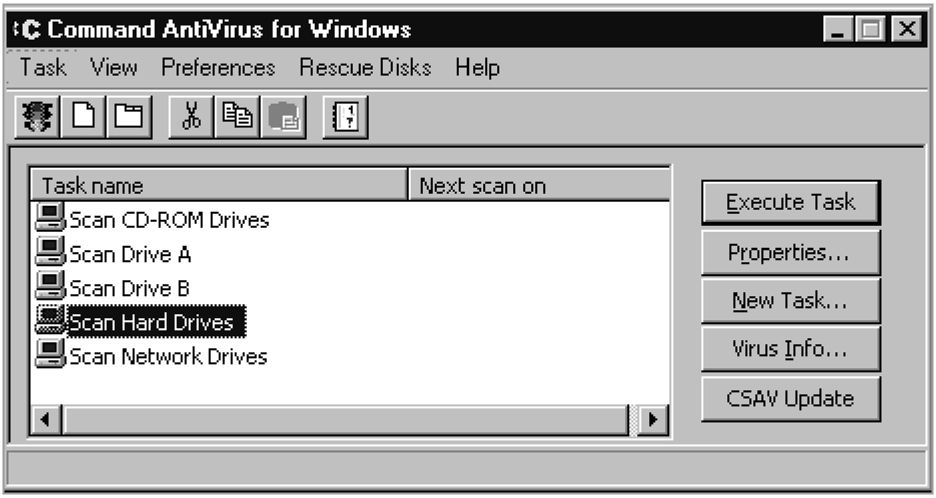
- You are a member of the Administrators group on the local machine
- System policy is set so that you have elevated privileges for installations
- Command AntiVirus has been advertised for the machine

2K/XP

- Command AntiVirus has been assigned through Group Policy

Although the program that checks to see if there are any updates to the Command AntiVirus administrative image runs when a user logs on, there may be times when it is necessary to start this program from within the GUI. For example, to make sure that you are protected from a new virus threat, you may need to have the users update virus definition files immediately.

The **CSAV Update** button in the **Command AntiVirus Main** dialog box allows a user on the network to start this program on-demand:



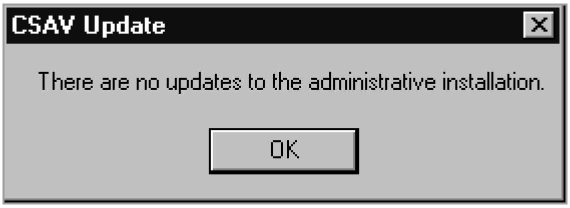
Task name	Next scan on
Scan CD-ROM Drives	
Scan Drive A	
Scan Drive B	
Scan Hard Drives	
Scan Network Drives	

Command AntiVirus Main Dialog Box

To start the updating agent, in the **Command AntiVirus Main** dialog box, click the **CSAV Update** button.

If the administrative image has been updated, the Command AntiVirus files are updated.

If the administrative image has **not** been updated, the system displays a **CSAV Update** message box informing you that there are no updates to the administrative image:



There are no updates to the administrative installation.

CSAV Update Message Box

Click **OK** to close the message box.

Scheduling the Update Agent on a Server

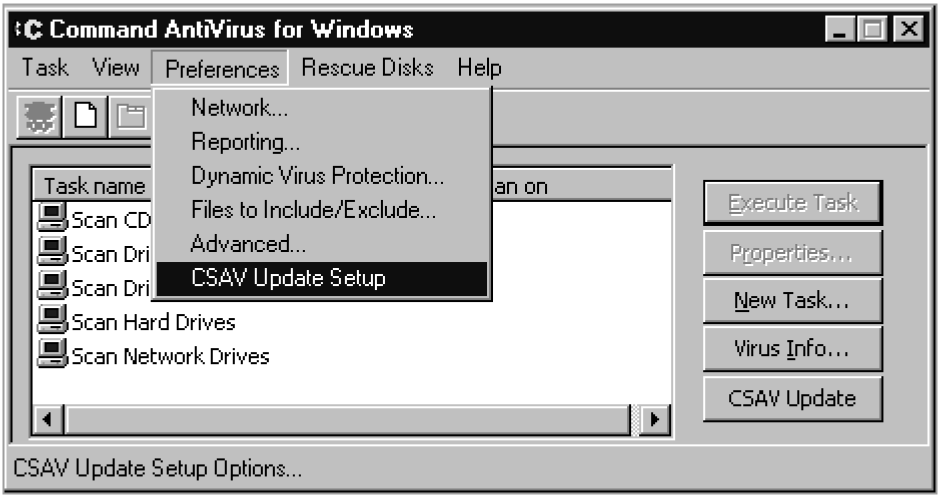
In Windows NT, Windows 2000, or Windows XP, to schedule the update agent, you **must** be authorized to access the centralized image, to install the software, and to schedule a task.

To make sure that Command AntiVirus installed on a server is kept up-to-date, you may want to schedule the start of the program (**CUAGENT.EXE)** that checks to see if there are any Command AntiVirus updates.

The **Preferences**/**CSAV Update Setup** menu item, allows administrators to schedule the update agent to run at a particular time.

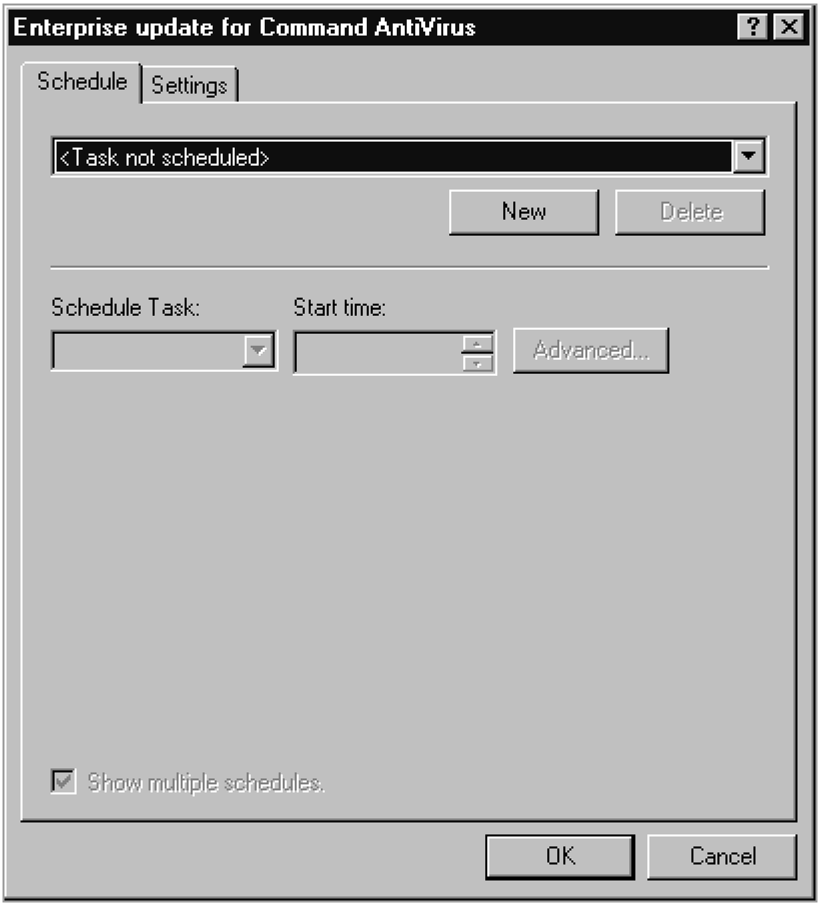
To schedule the update agent, follow these steps:

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



Preferences Menu

2. Click **CSAV Update Setup**. The system displays the **Enterprise Update for Command AntiVirus** dialog box with the **Schedule** dialog box in view:

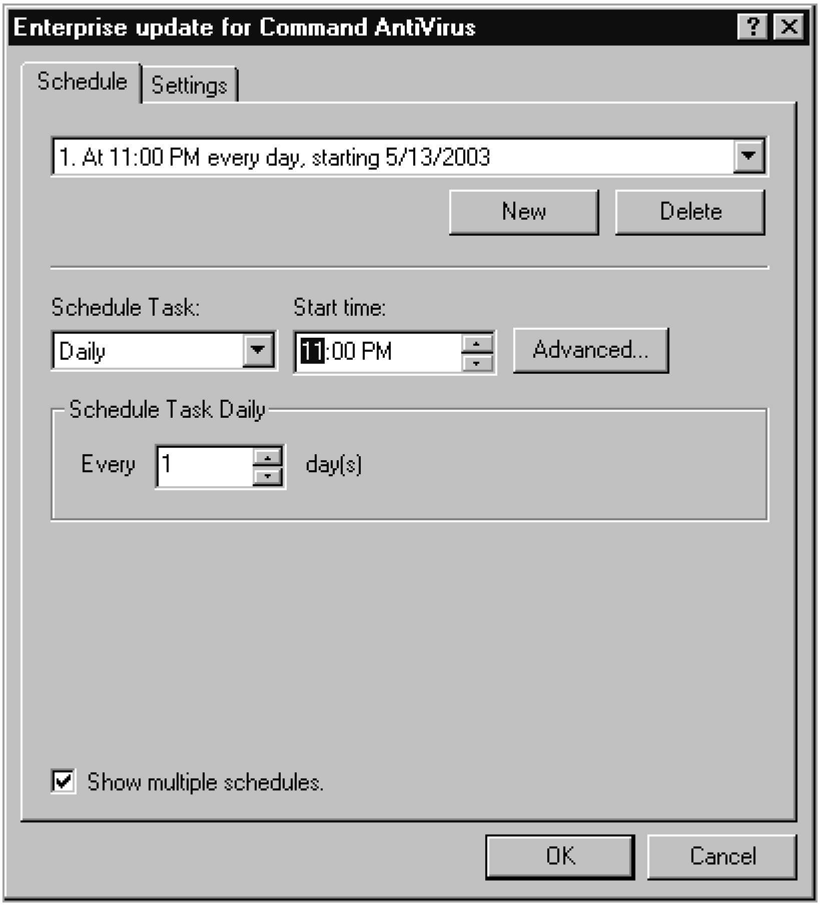


<Task not scheduled>

☑ Show multiple schedules.

Schedule Dialog Box

3. In the **Schedule** dialog box, click **New**. The new task is displayed in the task list box:


Enterprise update for Command AntiVirus

1. At 11:00 PM every day, starting 5/13/2003

Schedule Task: Daily

Start time: 11:00 PM

Schedule Task Daily

Every 1 day(s)

☑ Show multiple schedules.

Schedule Dialog Box

4. In the **Schedule Task** list, click the drop-down arrow, and select how frequently you want to start **CUAGENT**, for example, **Daily**, **Weekly**, **Monthly**, etc.

5. Depending on the selection that you made in **Step 4**, make the appropriate selections under **Schedule Task XXX**. For example, if you selected **Daily**, under **Schedule Task Daily**, select how many days you want **CUAGENT** to start, everyday, every two days, etc.
6. In the **Start time** box, click the **up** or **down** arrows to select the time of day that you want **CUAGENT** to start, for example 11:00 p.m.
7. Click **OK**. The system displays the Windows **Set Account Information** dialog box.

✓ **NOTE:** This account must have permission to read the SPD on the network as well as install updates.

8. Fill in your account information, and click **OK**. The system returns to the **Command AntiVirus Main** dialog box.

INTERNET UPDATE FEATURE

✓ **NOTE:** The **Internet Update** feature is <u>**not**</u> installed by default. You must install this feature during installation. For more information, refer to the ***Installation*** chapter of this guide.

In the **Internet Update**, users 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, they can set the **Update Now** feature to check for updates automatically.

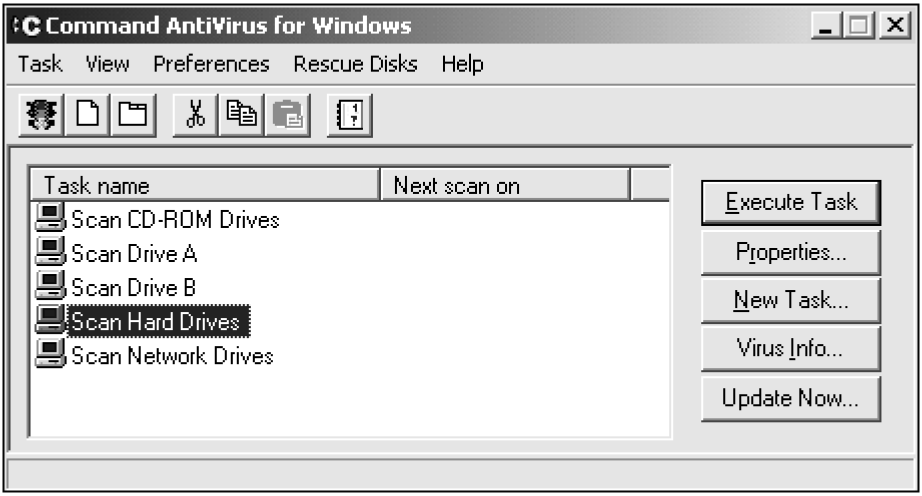
This section contains information on how to update Command AntiVirus on-demand. It also contains information on how to set Command AntiVirus to notify you when updates are available and what to do when you are notified.

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:

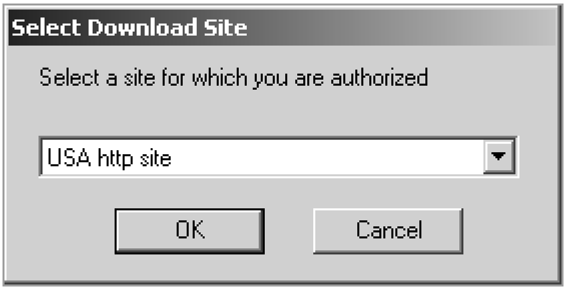


Task name	Next scan on
Scan CD-ROM Drives	
Scan Drive A	
Scan Drive B	
Scan Hard Drives	
Scan Network Drives	

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:



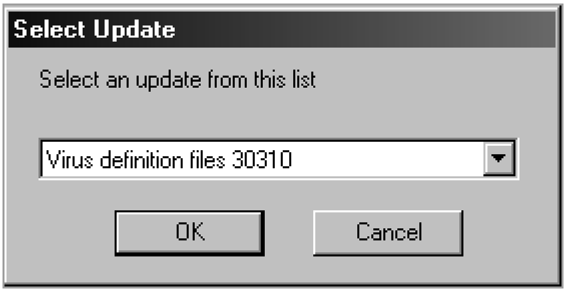
Select Download Site

Select a site for which you are authorized

USA http site

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

Select an update from this list

Virus definition files 30310

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.

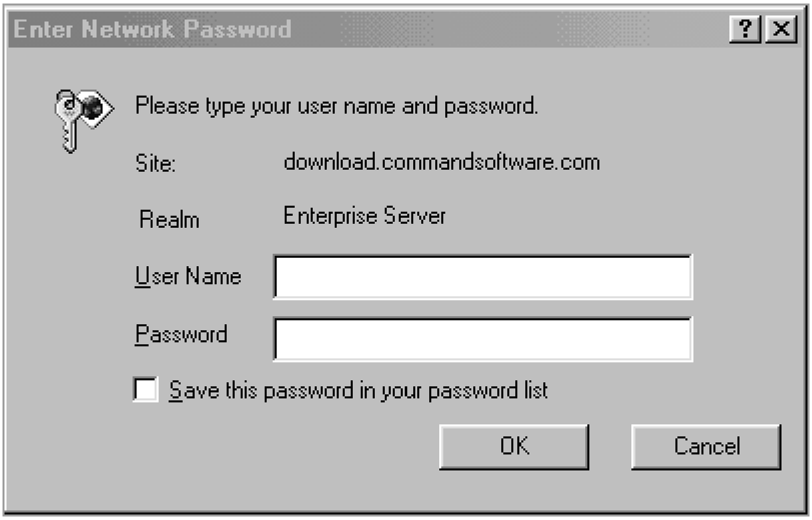
4. From the drop-down list, select the update or upgrade that you want to install. Available updates can include:

- **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

Please type your user name and password.

Site: download.commandsoftware.com

Realm Enterprise Server

User Name

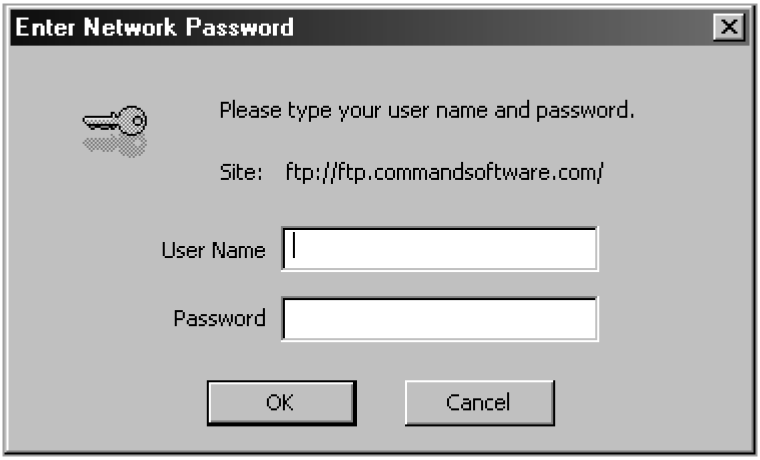
Password

□ Save this password in your password list

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** Command 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

Please type your user name and password.

Site: ftp://ftp.commandsoftware.com/

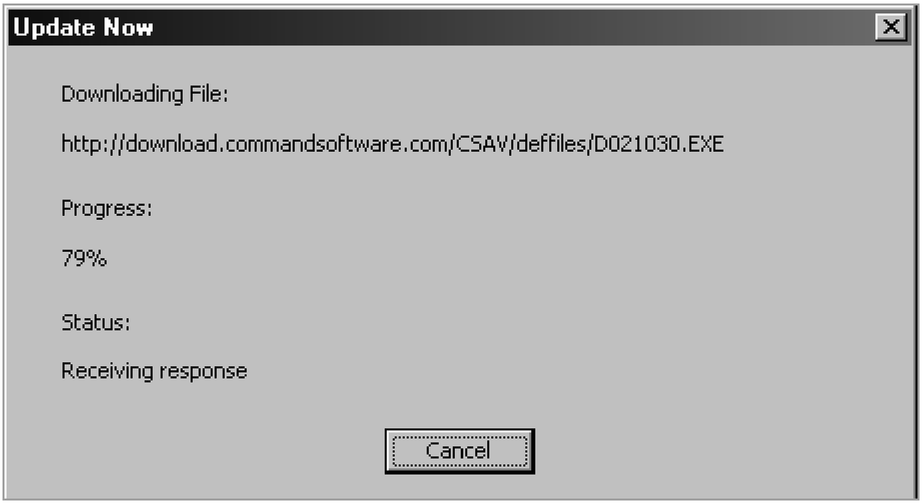
User Name

Password

Enter Network Password Dialog Box – FTP Site

This dialog box does **<u>not</u>** 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:



Downloading File:

http://download.commandsoftware.com/CSAV/deffiles/D021030.EXE

Progress:

79%

Status:

Receiving response

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.

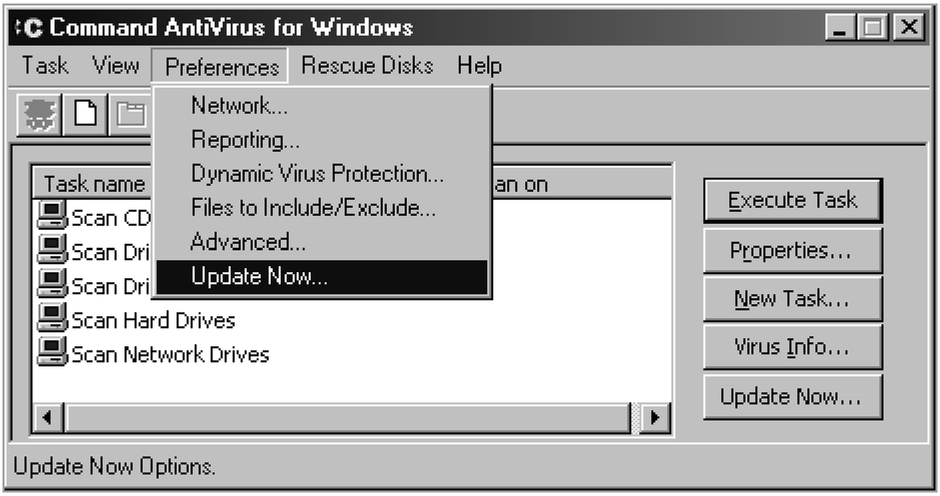
- **Sites** – Allows you to select the site from which you download the updated files. This dialog box also allows you to specify your Command user name and password for the download site and for any proxy server that you may use.
- **Updates** – Allows you to set Command AntiVirus to check for virus 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

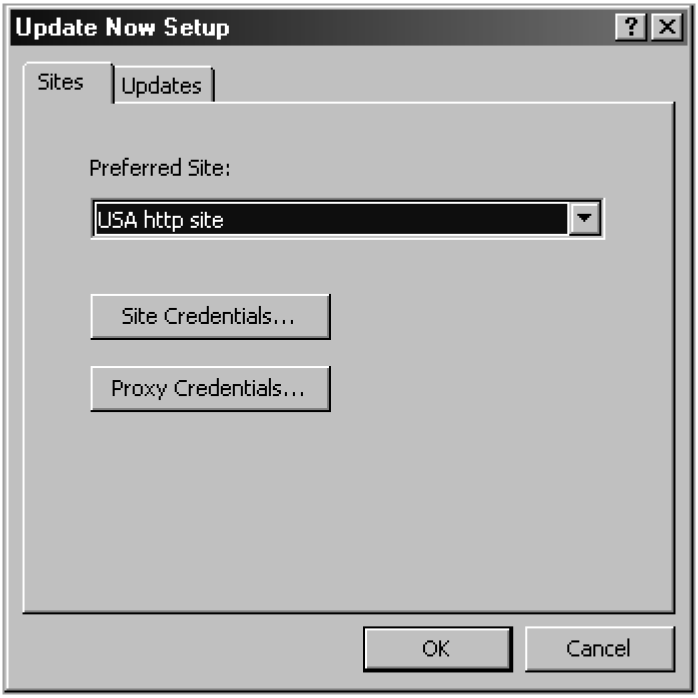
To set Command AntiVirus to check for updates and/or upgrades automatically, follow these steps:

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



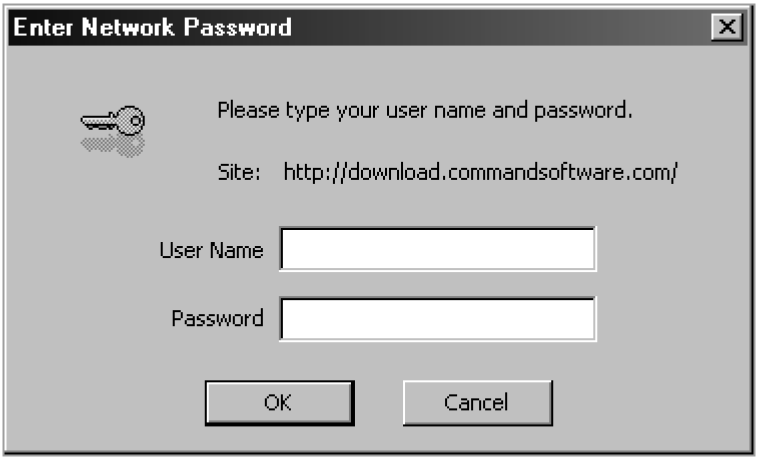
Preferences Menu

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

Please type your user name and password.

Site: http://download.commandsoftware.com/

User Name

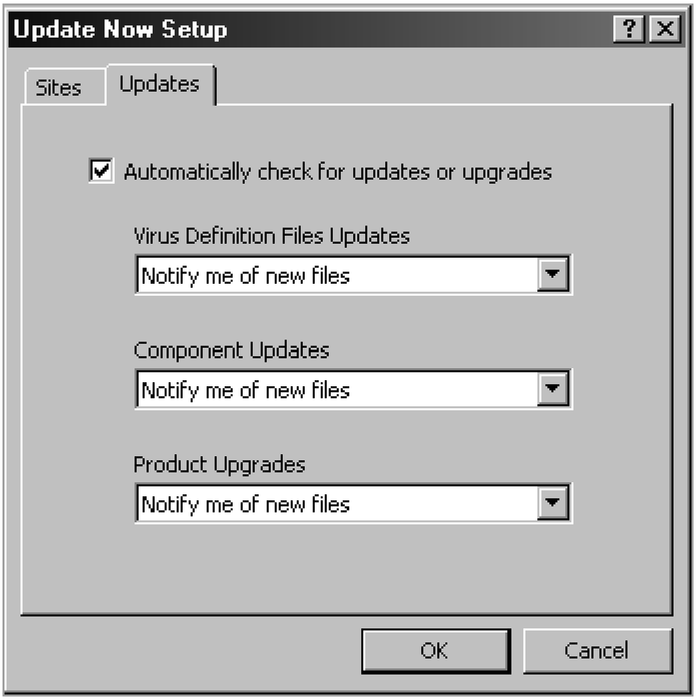
Password

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 **<u>not</u>** 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:



☑ Automatically check for updates or upgrades

Virus Definition Files Updates
Notify me of new files

Component Updates
Notify me of new files

Product Upgrades
Notify me of new files

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 **<u>only</u>** 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.

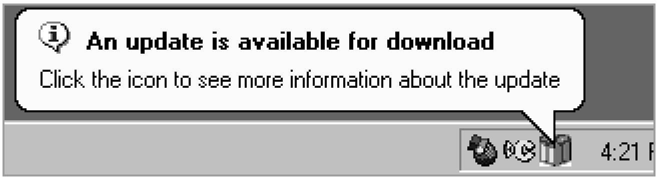
Download available

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:



An update is available for download

Click the icon to see more information about the update

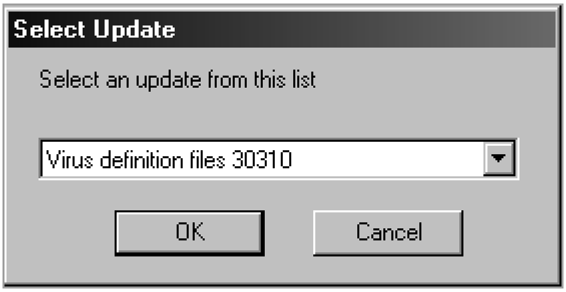
Download Available Balloon ToolTip

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

Select an update from this list

Virus definition files 30310

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.

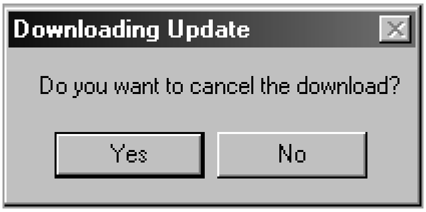
NOTE: If the program that displays the icons is stopped, the icon disappears until the following day when you log on to your computer.

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

Do you want to cancel the download?

Downloading Update Dialog Box

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

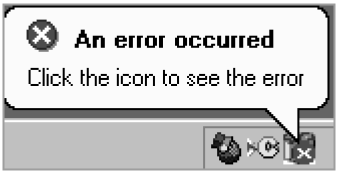
Download error

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:



An error occurred

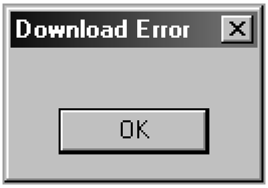
Click the icon to see the error

Download Error Balloon ToolTip

Understanding Why the Download Failed

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

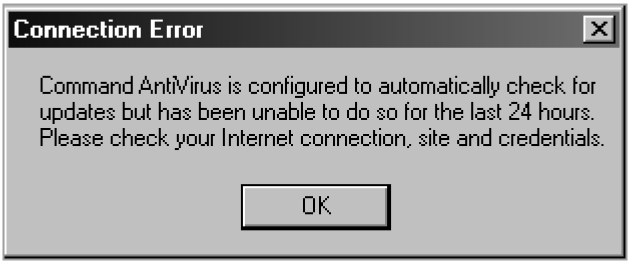
1. In the Windows notification area, click the **Download error** icon .
   The system displays the **Download error** message box:



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:



Command AntiVirus is configured to automatically check for updates but has been unable to do so for the last 24 hours. Please check your Internet connection, site and credentials.

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.

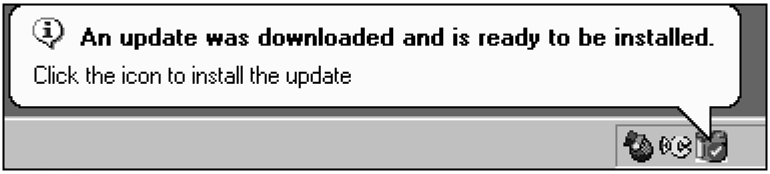
Update ready to install

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:



An update was downloaded and is ready to be installed.

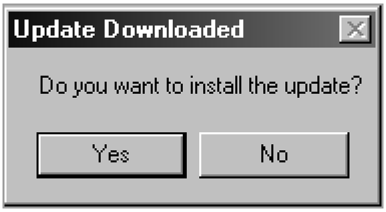
Click the icon to install the update

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

Do you want to install the update?

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.

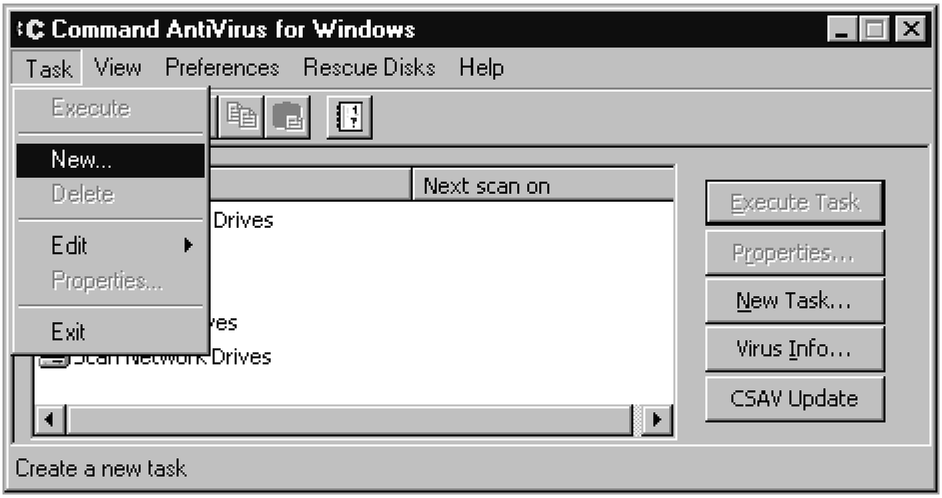
CREATING A NEW SCAN TASK

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:

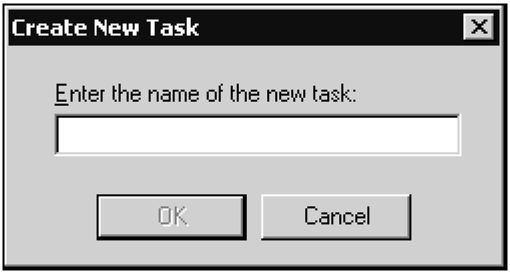
1. On the Command AntiVirus menu bar, click **Task.** The system displays the **Task** menu:



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.

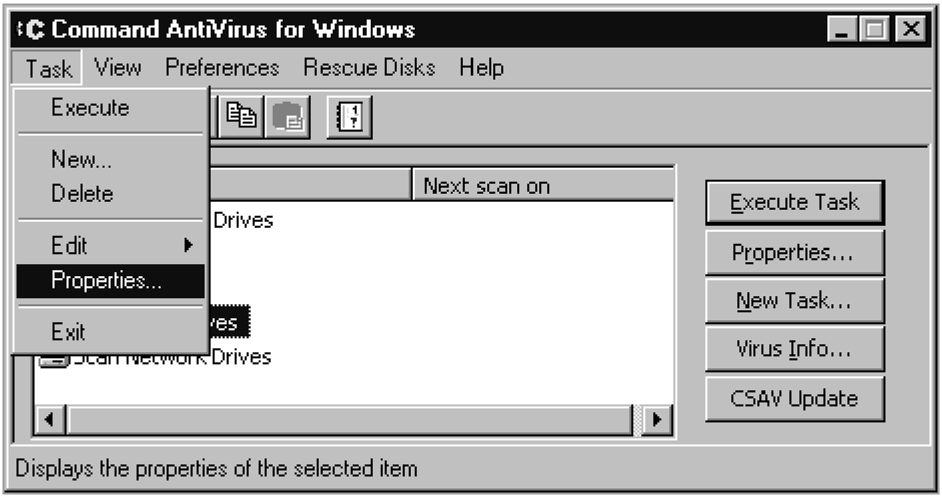
The **Properties – *Name of Scan Task*** dialog box contains the **Properties** and **Advanced Properties** dialog boxes that allow you to set the scanning properties of a scan task. Each of these dialog boxes are identified by a name tab.

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:

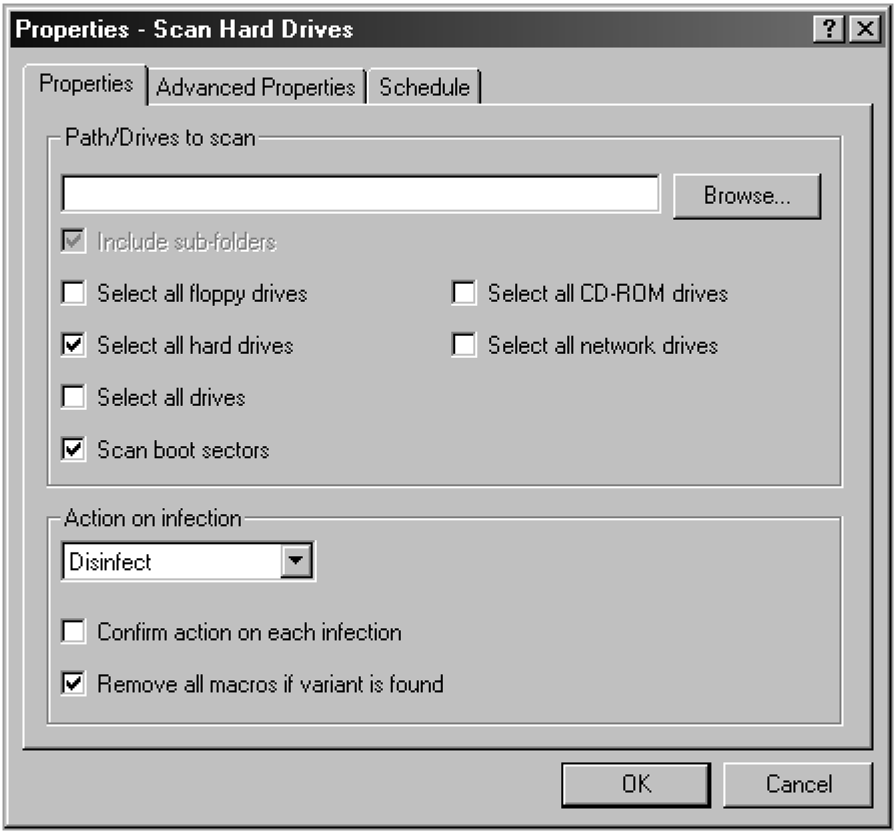


Displays the properties of the selected item

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.



Path/Drives to scan

☑ Include sub-folders

□ Select all floppy drives

□ Select all CD-ROM drives

☑ Select all hard drives

□ Select all network drives

□ Select all drives

☑ Scan boot sectors

Action on infection

Disinfect

□ Confirm action on each infection

☑ Remove all macros if variant is found

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.

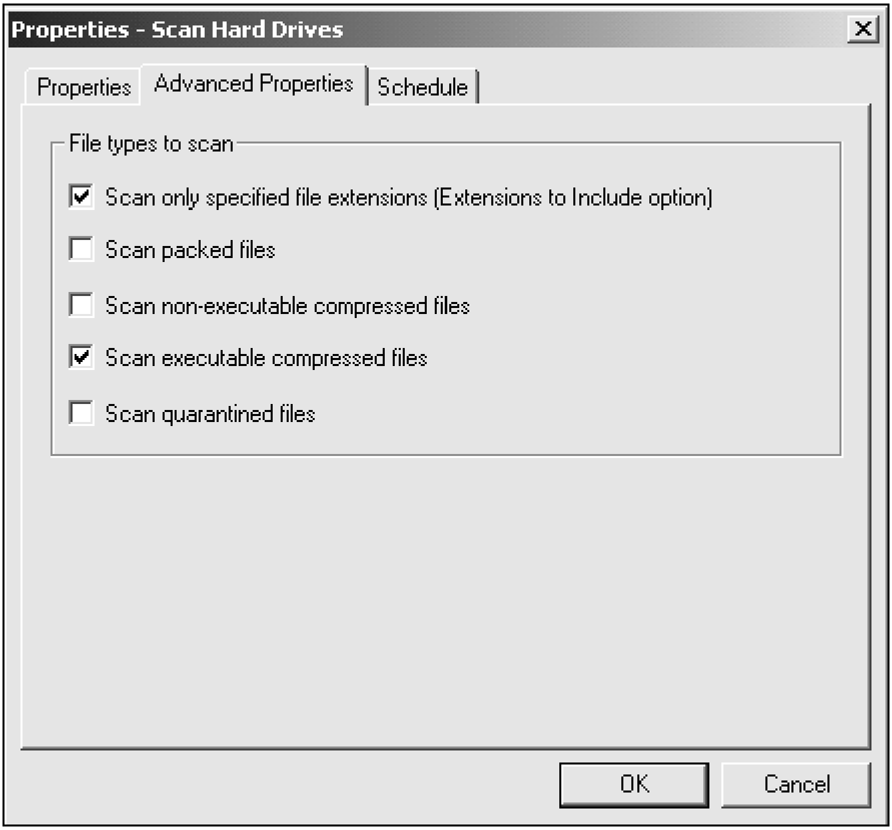
  For more information, refer to **Using the Quarantine Feature** located later in this chapter.

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:



Properties - Scan Hard Drives

File types to scan

☑ Scan only specified file extensions (Extensions to Include option)

☐ Scan packed files

☐ Scan non-executable compressed files

☑ Scan executable compressed files

☐ Scan quarantined files

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 **<u>not</u>** selected, the quarantine folder is **<u>not</u>** 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 **<u>cannot</u>** 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 **<u>not</u>** signed on as a member of the Administrators group on the local machine, you **<u>cannot</u>** cut a **System Task**.

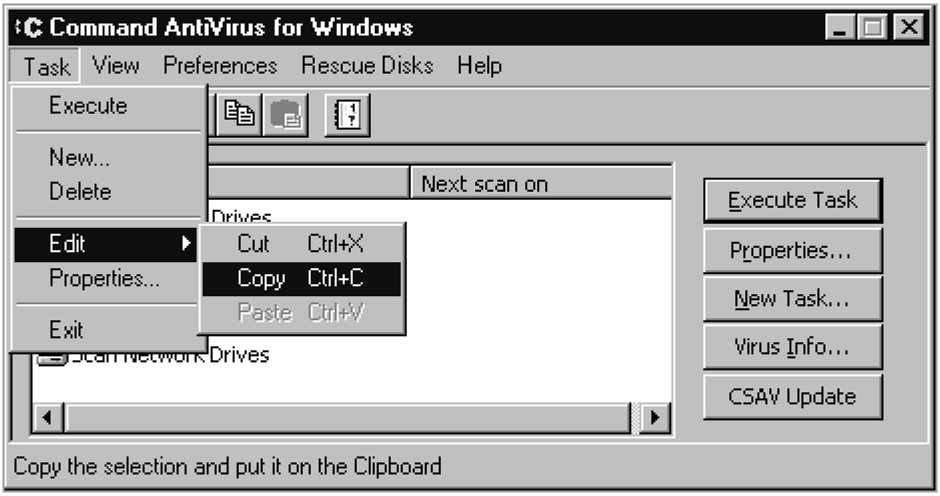
If you are signed on as a member of the Administrators group on the local machine and you copy and paste a **System Task**, the task remains a **System Task**.

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:



Copy the selection and put it on the Clipboard

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

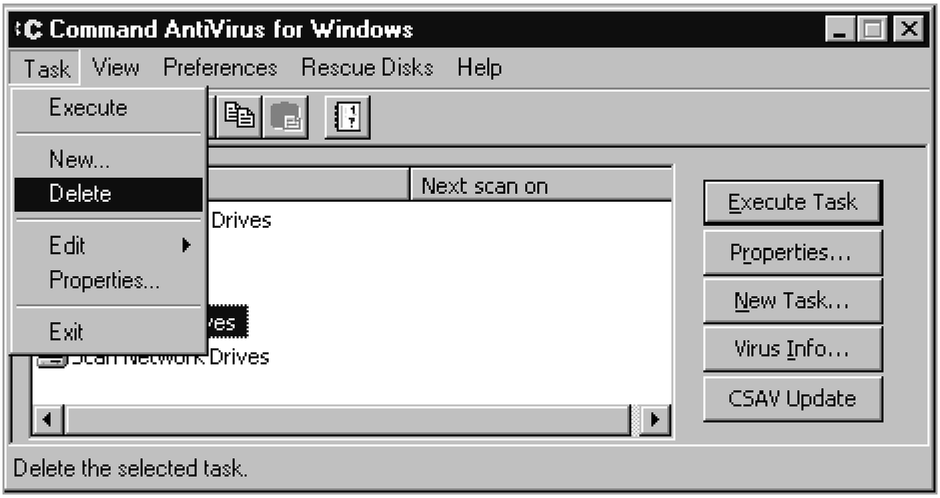
NT/2K/XP

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:



Delete the selected task.

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.

NT/2K/XP

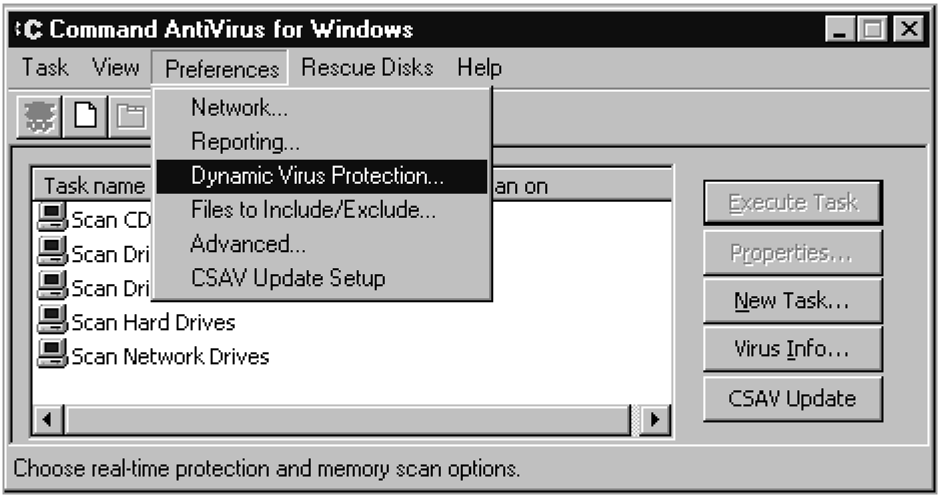
In Windows NT, Windows 2000, and Windows XP, to change **Preferences**, you **must** be signed on as a member of the Administrators group on the local machine. If you are not, all of the menu items except **Advanced** are available **only** for viewing.

Administrators can enable this option by using the Custom Installation Wizard for Command AntiVirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this administrator’s guide.

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:

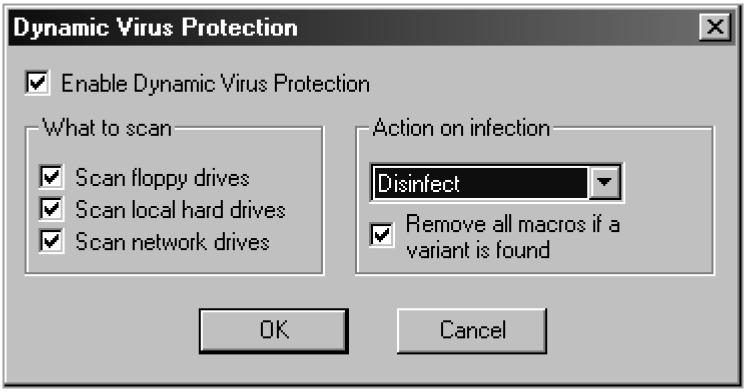
1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Choose real-time protection and memory scan options.

Preferences Menu

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



☑ Enable Dynamic Virus Protection

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

Disinfect

☑ Remove all macros if a variant is found

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.

NT/2K/XP

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.

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.

Administrators can enable this option by using the Custom Installation Wizard for Command AntiVirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this guide.

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.

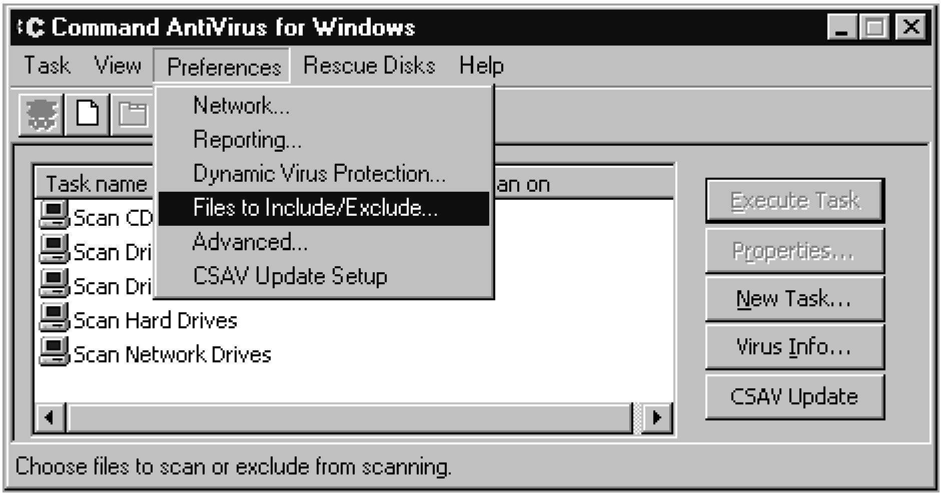
NOTE: Command AntiVirus does **not** scan self-extracting files by default. Dynamic Virus Protection (DVP) scans the contents of the self-extracting file when the files are extracted. However, the .EXE portion of the self-extracting file is scanned by default.

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:

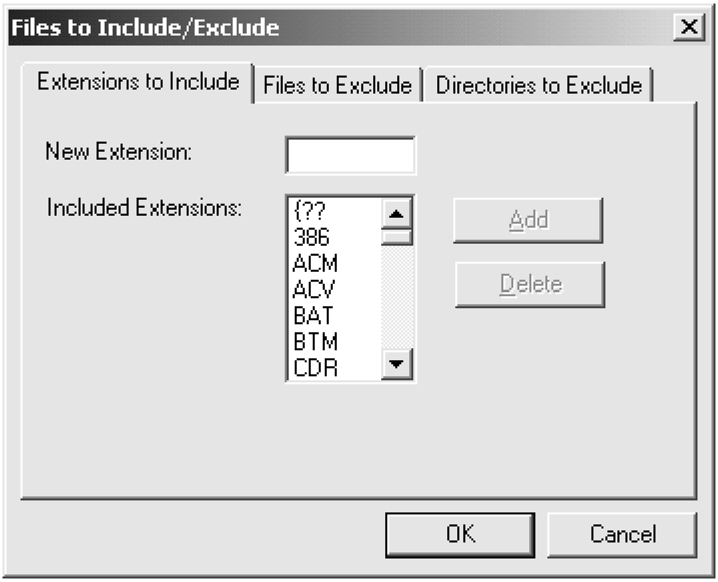
1. On the Command AntiVirus menu bar, click **Preferences**. The system displays the **Preferences** menu:



Choose files to scan or exclude from scanning.

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.

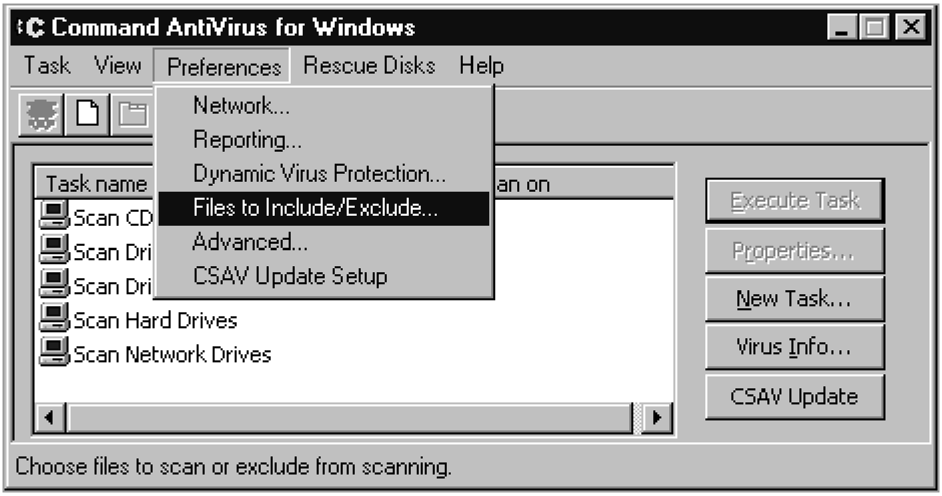
SPECIFYING FILES TO EXCLUDE FROM SCANS

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:



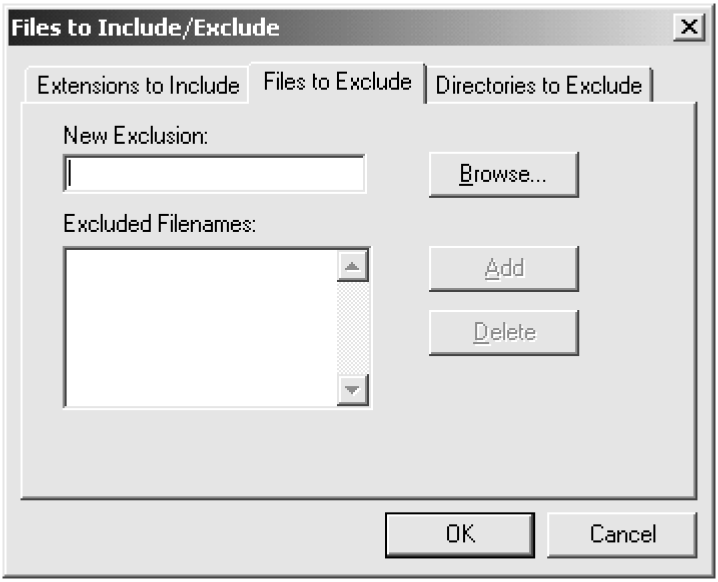
Choose files to scan or exclude from scanning.

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.

USING COMMAND ANTIVIRUS

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



Files to Exclude Dialog Box

4. 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.

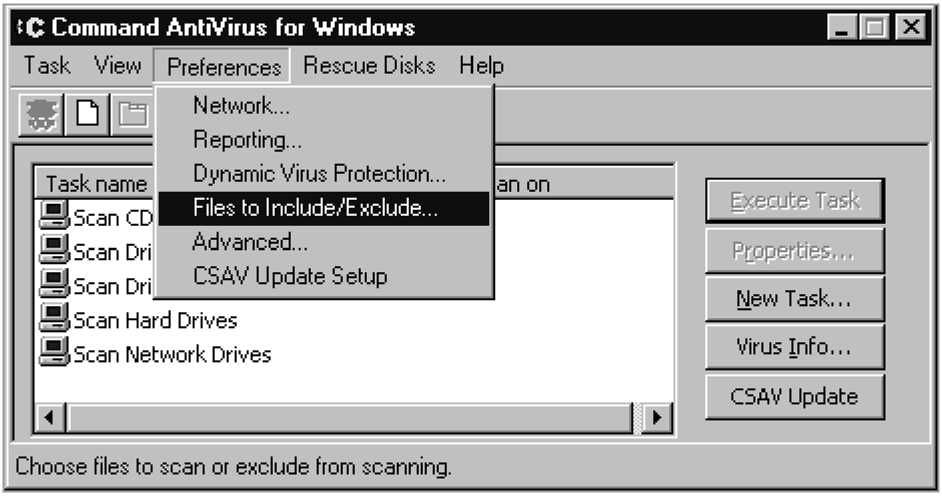
As the potential of excluding directories that may contain a virus infection exists, we recommend that you use this option with caution.

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:

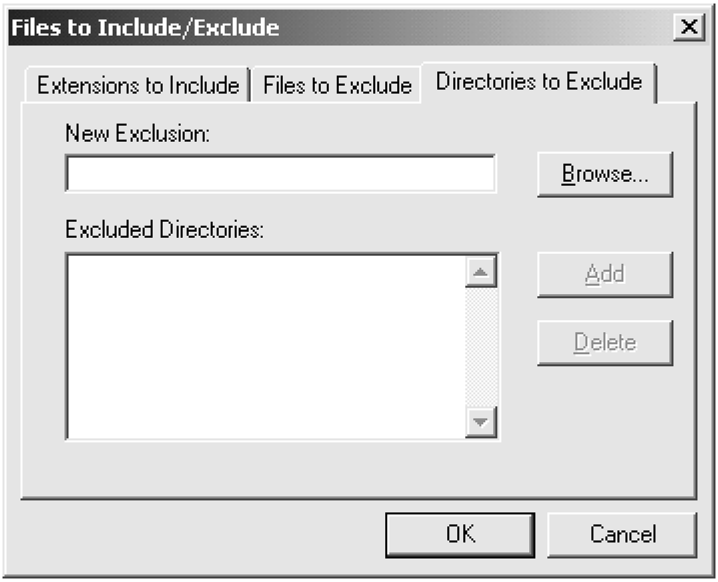


Choose files to scan or exclude from scanning.

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.

Administrators can enable this option by using the Custom Installation Wizard for Command AntiVirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this administrator’s guide.

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:

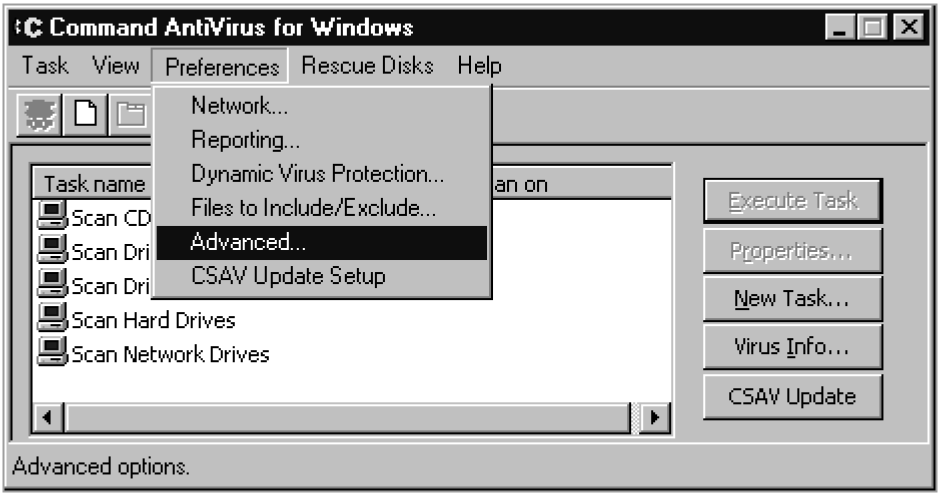
```
C:\CSAV_quarantine
```

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.

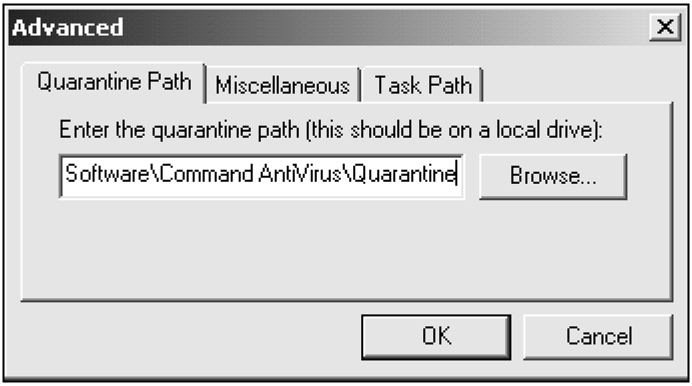
To set the path to the quarantine folder, follow these steps:

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:



Enter the quarantine path (this should be on a local drive):

Software\Command AntiVirus\Quarantine

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

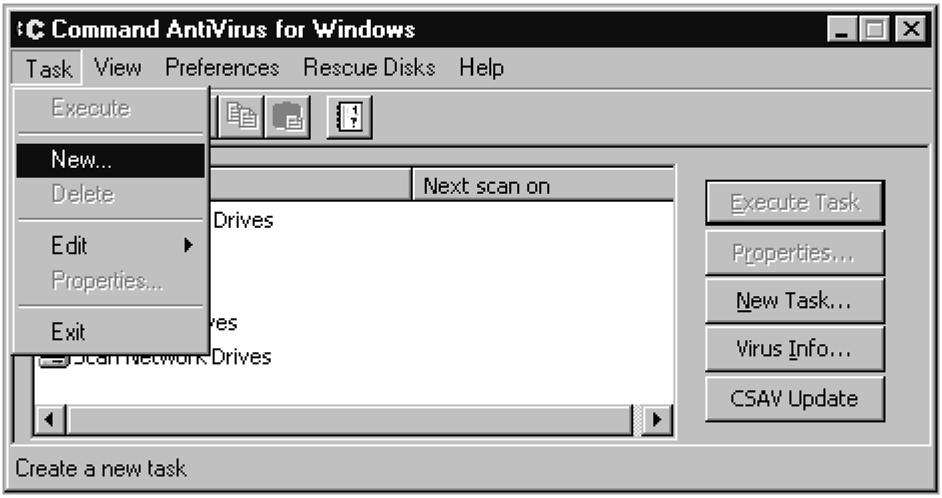
You can create a scan task that disinfects infected files that are stored in the quarantine folder.

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

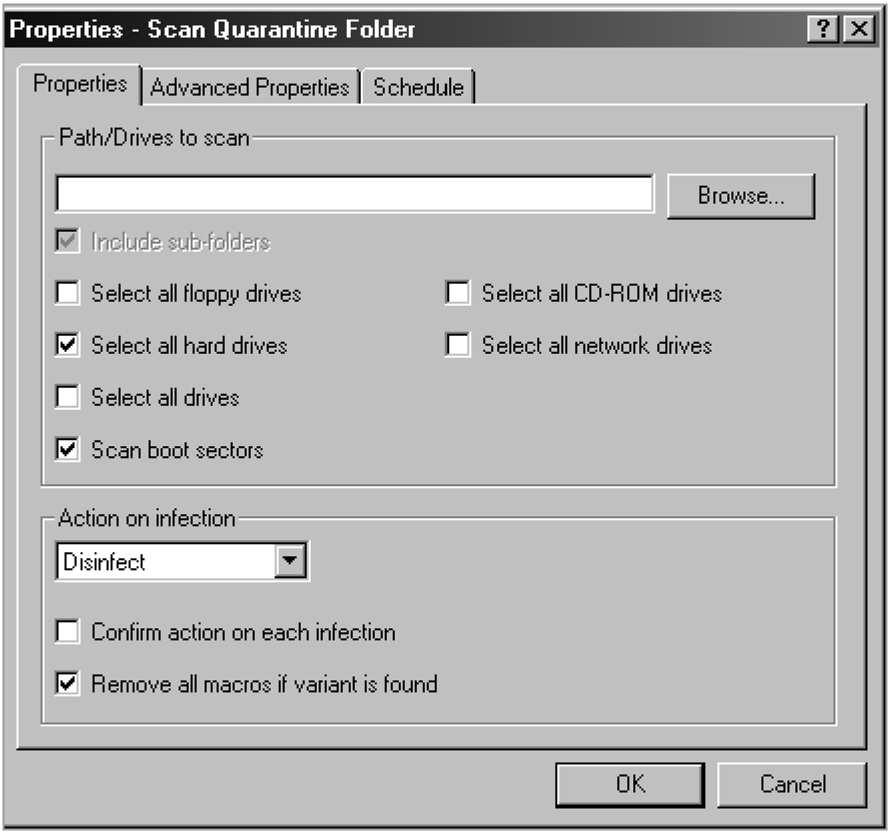
2. Select **New**. The system displays a **Create New Task** dialog box.

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:



Path/Drives to scan

☑ Include sub-folders

□ Select all floppy drives

□ Select all CD-ROM drives

☑ Select all hard drives

□ Select all network drives

□ Select all drives

☑ Scan boot sectors

Action on infection

Disinfect

□ Confirm action on each infection

☑ Remove all macros if variant is found

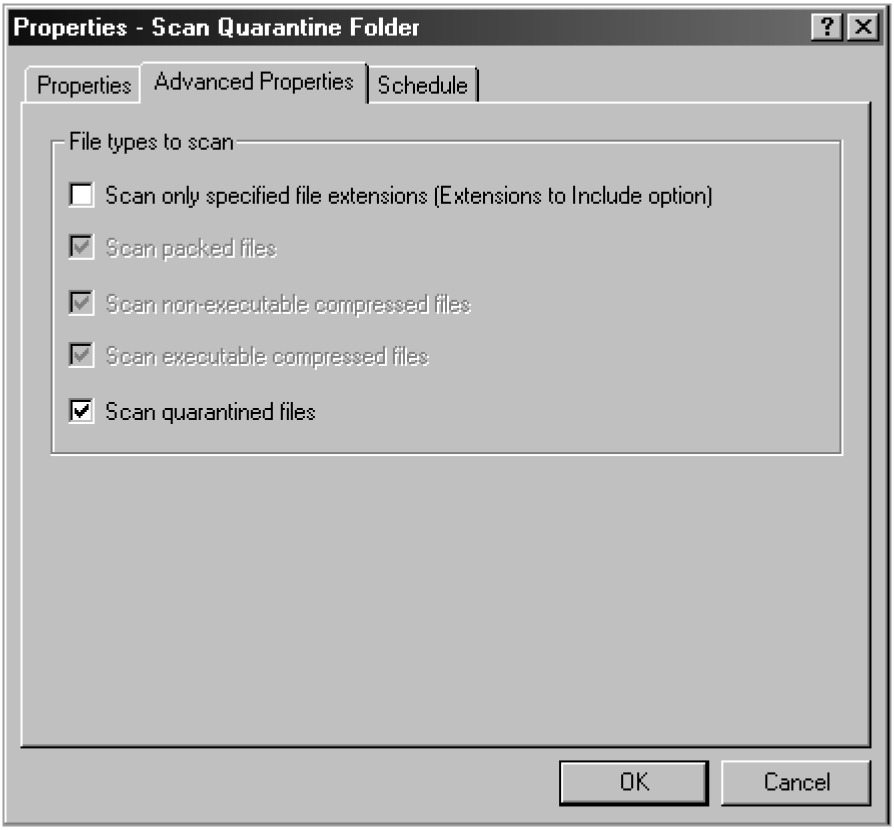
Properties Dialog Box

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**.

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



Properties - Scan Quarantine Folder

File types to scan

☐ Scan only specified file extensions (Extensions to Include option)

☑ Scan packed files

☑ Scan non-executable compressed files

☑ Scan executable compressed files

☑ Scan quarantined files

Advanced Properties Dialog Box

8. Under **File types to scan**, clear the **Scan only specified file extensions (Extensions to Include option)** to select all files.
9. Select the **Scan quarantined files** check box.
10. 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 **<u>must</u>** rename the files to their original names and move the files back to their original locations.

NOTE: If for some reason a file was **<u>not</u>** 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 **<u>not</u>** 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.

In Windows NT, Windows 2000, and Windows XP, to change **Preferences**, you **<u>must</u>** 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 **<u>only</u>** for viewing.

Administrators can enable this option by using the Custom Installation Wizard for Command AntiVirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this administrator’s guide.

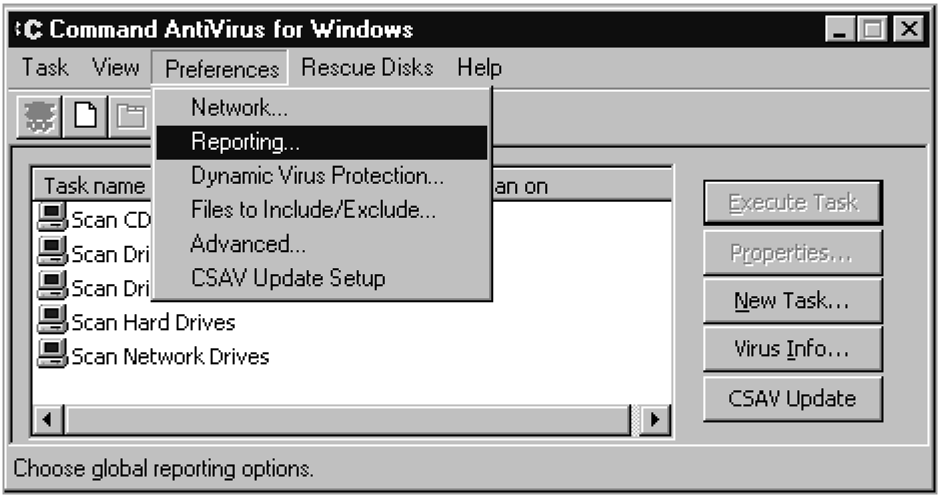
NOTE: As you can send a virus report at the end of a manual scan, this **E-mail** option does **not** apply to manual scans.

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.

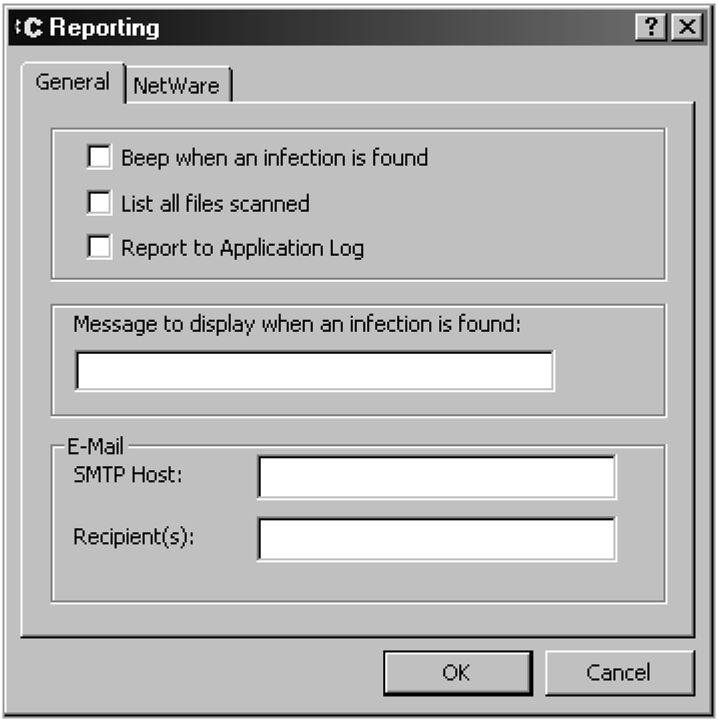
To set up sending a virus notification e-mail, follow these steps:

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:



□ Beep when an infection is found

□ List all files scanned

□ Report to Application Log

Message to display when an infection is found:

E-Mail

SMTP Host:

Recipient(s):

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**.

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.

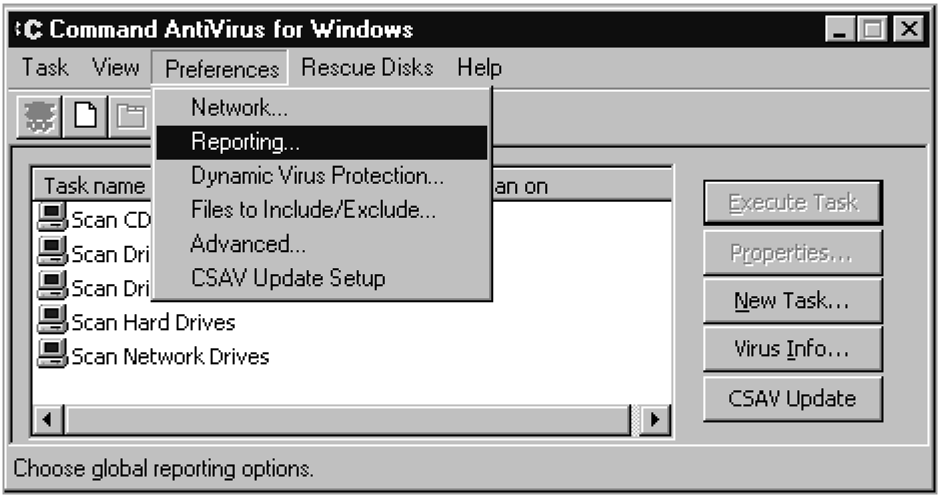
Administrators can enable this option by using the Custom Installation Wizard for Command AntiVirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this administrator's guide.

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:

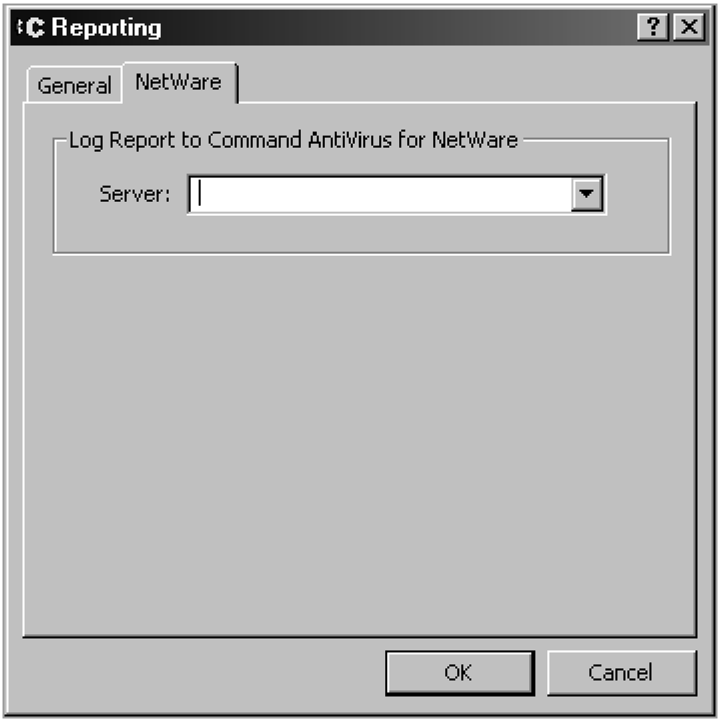


Choose global reporting options.

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.

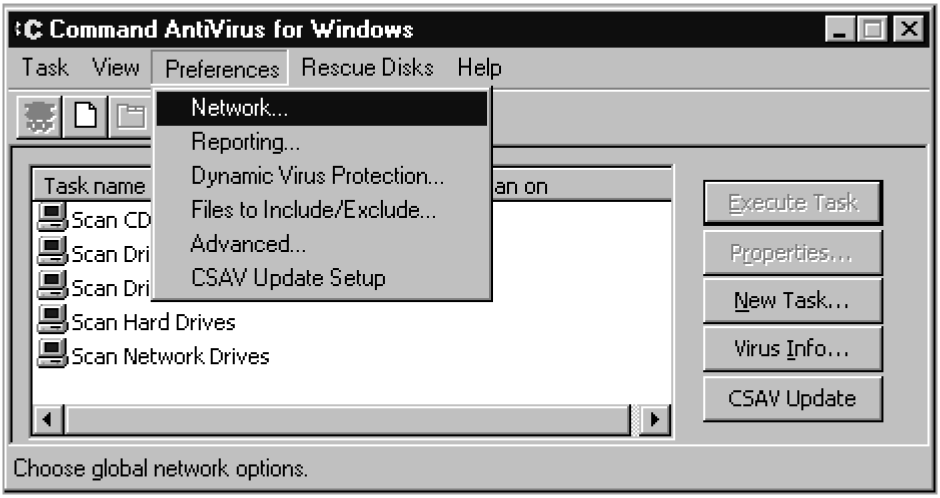
In Windows NT, Windows 2000, and Windows XP, to change **Preferences**, you **must** be signed on as a member of the Administrators group on the local machine. If you are not, all of the menu items except **Advanced** are available **only** for viewing.

Administrators can enable this option by using the Custom Installation Wizard for Command AntiVirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this administrator's guide.

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

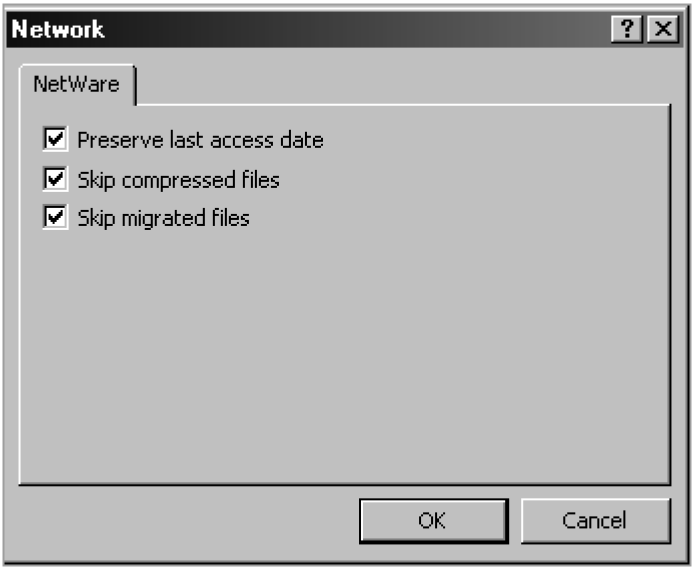
To set the scanning options for NetWare drives, follow these steps:

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:



☑ Preserve last access date

☑ Skip compressed files

☑ Skip migrated files

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.

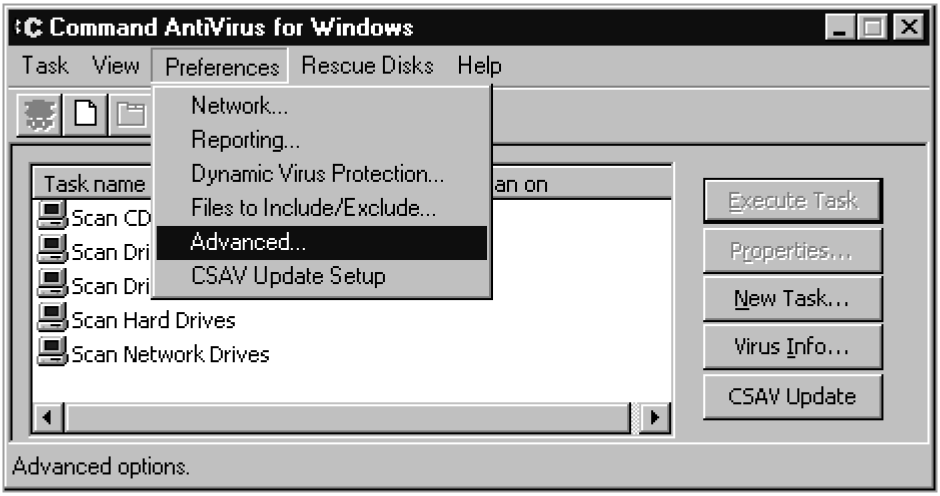
As a network administrator, you may want to change the folder that stores system scan tasks. For example, you may want to create a set of specific scan tasks for your users that are stored in a network folder to which they have access. You can specify the new path in the **Preferences/Advanced/Task Path**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

Administrators can enable this option by using the Custom Installation Wizard for Command AntiVirus or the System Policy Template for Command AntiVirus. For more information, refer to the ***COMMANDCentral*** chapter of this administrator's guide.

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

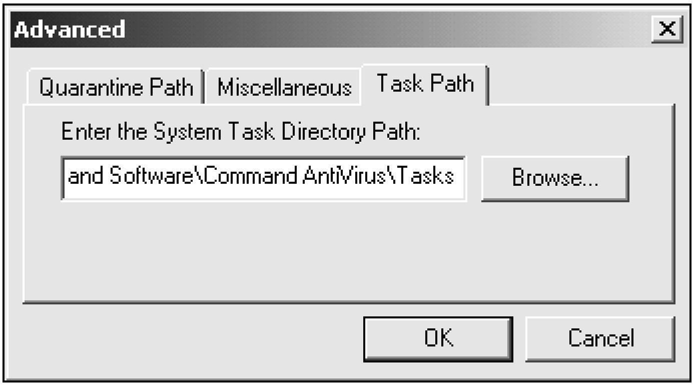
To change the default Command AntiVirus **System** scan task folder, follow these steps:

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:



Enter the System Task Directory Path:

and Software\Command AntiVirus\Tasks

Task Path Dialog Box

4. In the **Enter the System Task Directory Path** text box, type the full path to the new folder.

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

5. Click **OK**.

The **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.

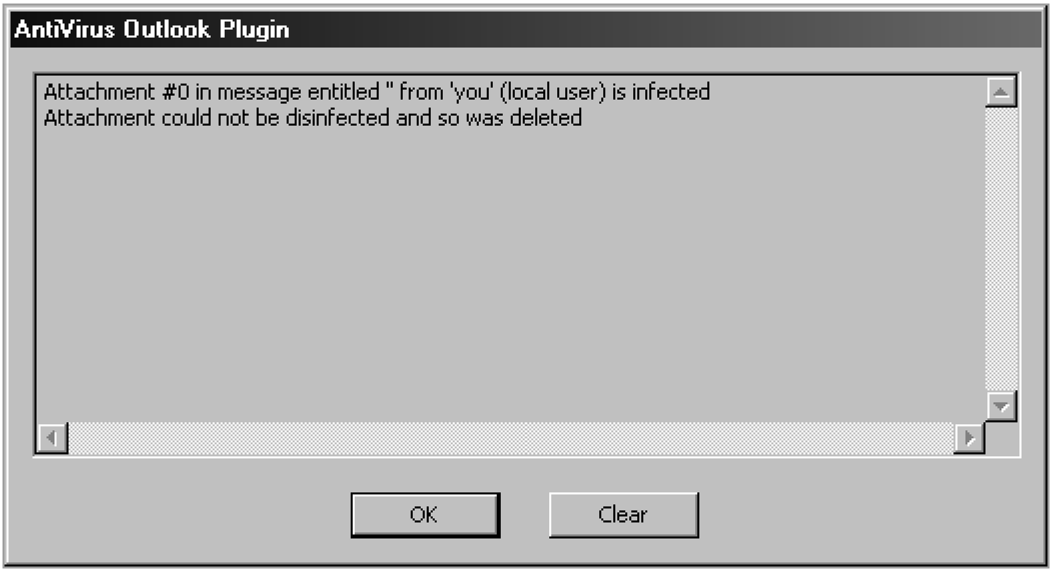
The Outlook Scanner is **not** installed by default. You must install this feature during installation or afterwards by using the installation program's **Application Maintenance** dialog box. For more information, refer to the ***Installation*** chapter of this guide.

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:

USING COMMAND ANTIVIRUS



Attachment #0 in message entitled '' from 'you' (local user) is infected
Attachment could not be disinfected and so was deleted

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

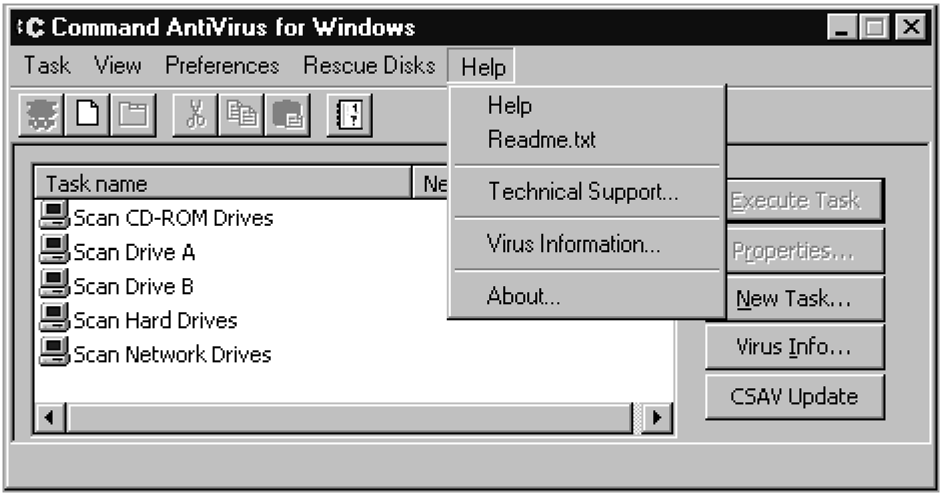
You can find the answers to many of your product-related questions through the **Help** menu. For example, you can find information on

- 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:

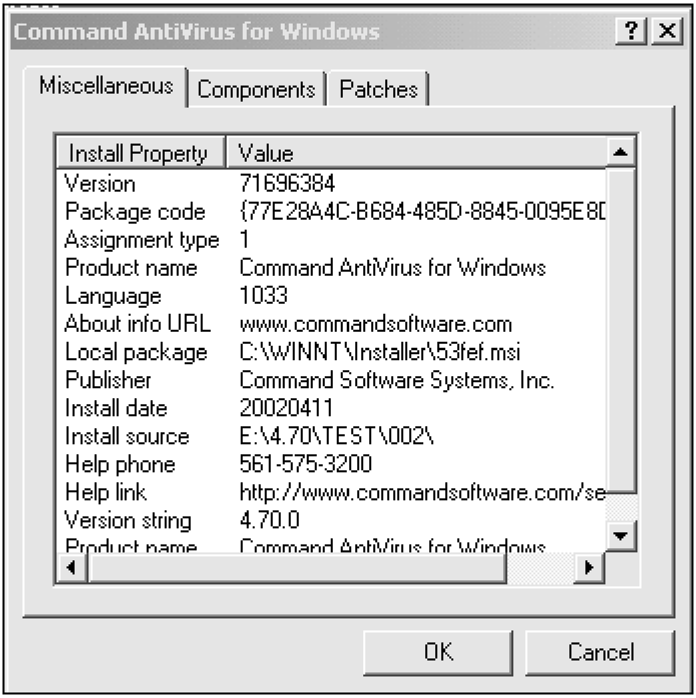
- Product version number
- Date of the scan engine
- Date of the **SIGN.DEF** definition file
- Date of the **SIGN2.DEF** definition file
- Date of the **MACRO.DEF** definition file
- Copyright information

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**.

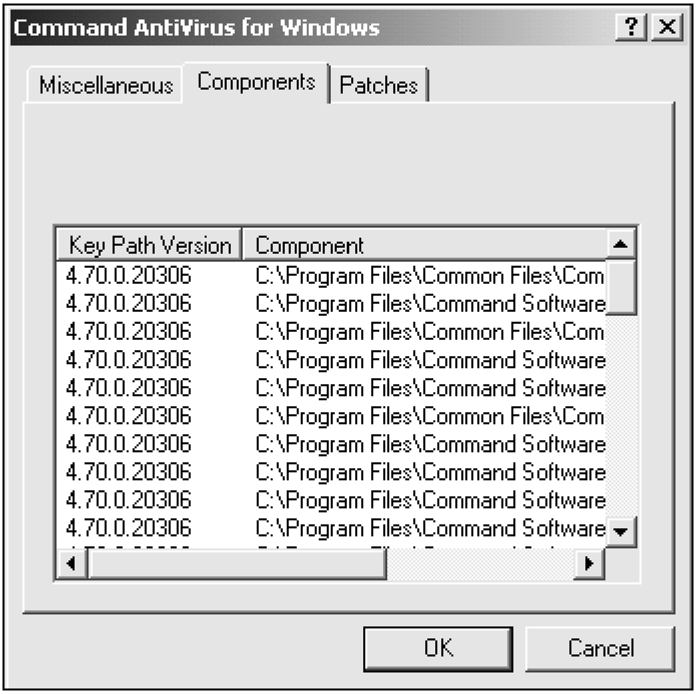
The **Miscellaneous** dialog box contains information that is specific to the currently installed version of the product. For example, it contains the name of the product, the date the product was installed, the location of the installation source, etc.:



Install Property	Value
Version	71696384
Package code	{77E28A4C-B684-485D-8845-0095E8D
Assignment type	1
Product name	Command AntiVirus for Windows
Language	1033
About info URL	www.commandsoftware.com
Local package	C:\WINNT\Installer\53fef.msi
Publisher	Command Software Systems, Inc.
Install date	20020411
Install source	E:\4.70\TEST\002\
Help phone	561-575-3200
Help link	http://www.commandsoftware.com/se
Version string	4.70.0
Product name	Command AntiVirus for Windows

Miscellaneous Dialog Box

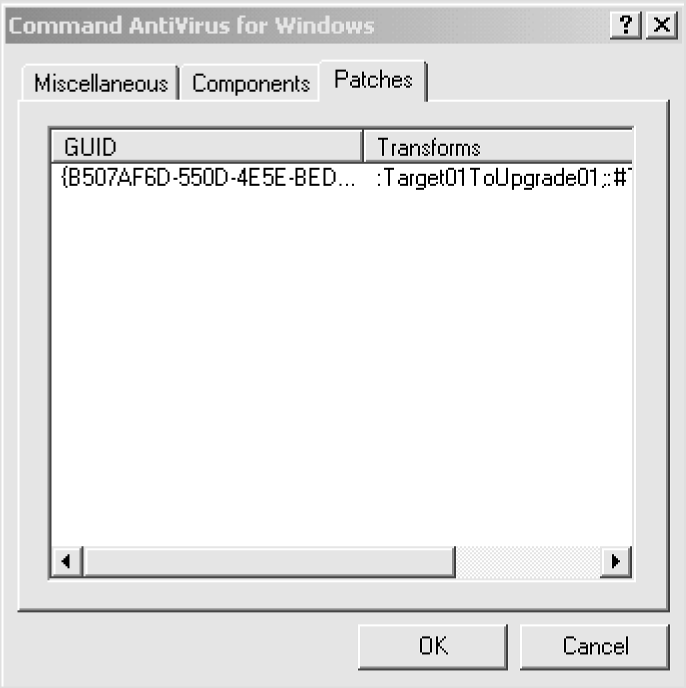
The **Components** dialog box contains the version number and the location of each installed component of the product:



Key Path Version	Component
4.70.0.20306	C:\Program Files\Common Files\Com
4.70.0.20306	C:\Program Files\Command Software
4.70.0.20306	C:\Program Files\Common Files\Com
4.70.0.20306	C:\Program Files\Command Software
4.70.0.20306	C:\Program Files\Command Software
4.70.0.20306	C:\Program Files\Common Files\Com
4.70.0.20306	C:\Program Files\Command Software
4.70.0.20306	C:\Program Files\Command Software
4.70.0.20306	C:\Program Files\Command Software
4.70.0.20306	C:\Program Files\Command Software

Components Dialog Box

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



GUID	Transforms
{B507AF6D-550D-4E5E-BED...	:Target01ToUpgrade01;:#T

Patches Dialog Box

BOOT RECORD SUPPORT

4

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.

5

DOS RECOVERY

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

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

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

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

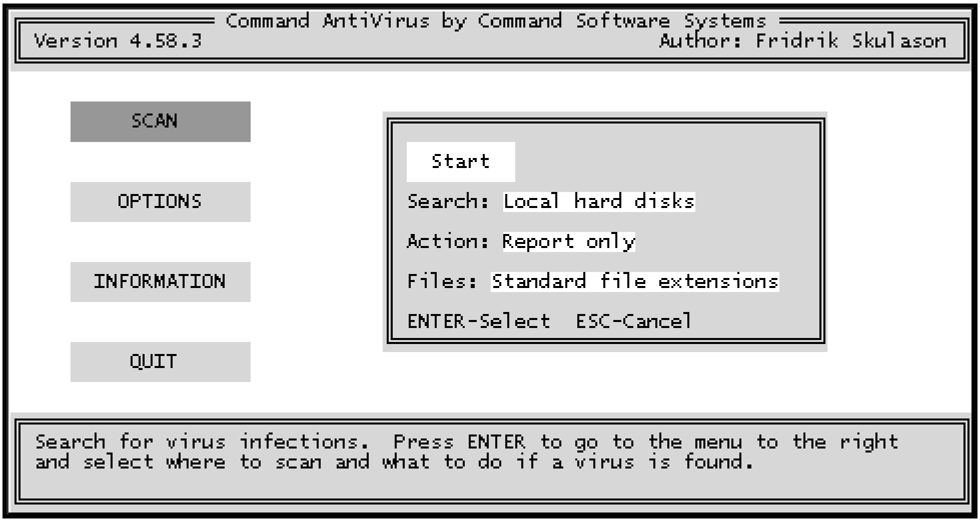
NOTE: For NTFS systems, unless you can access an NTFS drive from within DOS, for example, by using third party software, you will **not** be able to use the rescue disk set to scan files on an NTFS drive.

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

F-PROT.EXE MENU OPTIONS

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

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



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

Start
Search: Local hard disks
Action: Report only
Files: Standard file extensions
ENTER-Select  ESC-Cancel

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

Main Menu

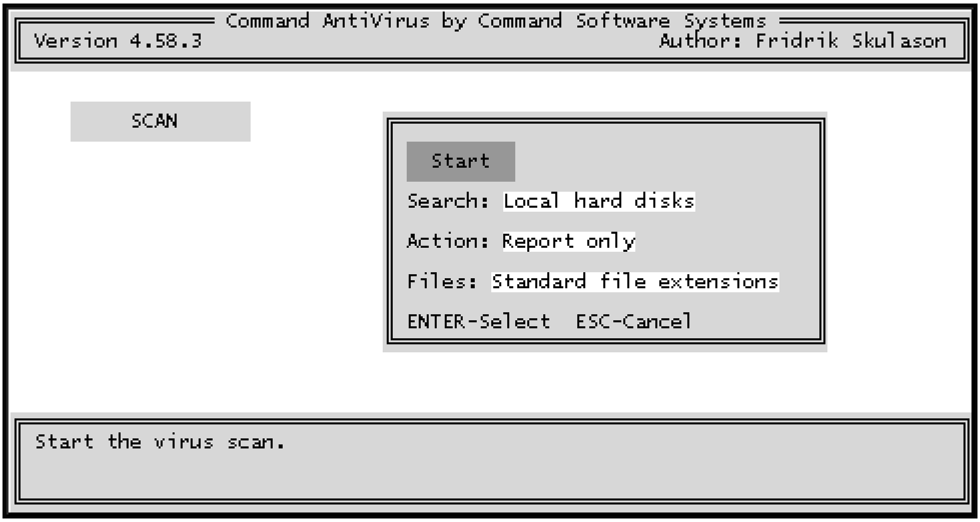
You can select an item from the menu by using the arrow keys to highlight the appropriate command and then pressing **Enter**.

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

The following section describes these items in detail.

SCAN

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



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

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

Start the virus scan.
```

Scan Menu

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

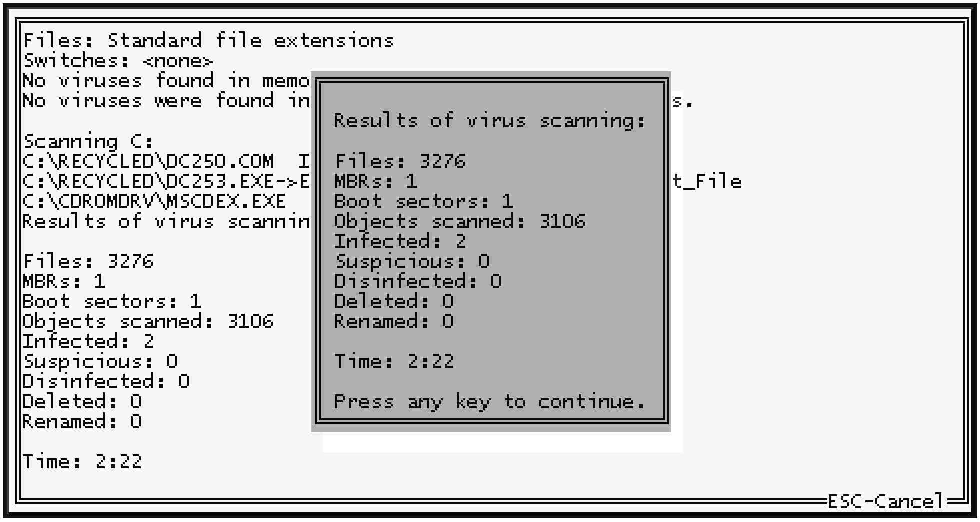
The following descriptions will help you decide which options to select.

Start

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

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

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



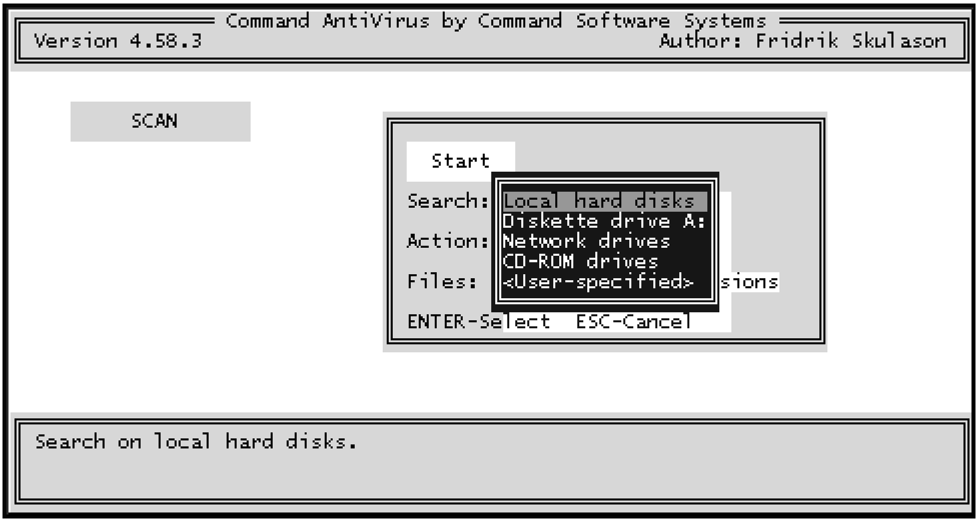
```
Files: Standard file extensions
Switches: <none>
No viruses found in memo
No viruses were found in                             s.
                          Results of virus scanning:
Scanning C:
C:\RECYCLED\DC250.COM  I  Files: 3276
C:\RECYCLED\DC253.EXE->E  MBRs: 1                    t_File
C:\CDROMDRV\MSCDEX.EXE    Boot sectors: 1
Results of virus scannin  Objects scanned: 3106
                          Infected: 2
Files: 3276               Suspicious: 0
MBRs: 1                   Disinfected: 0
Boot sectors: 1           Deleted: 0
Objects scanned: 3106     Renamed: 0
Infected: 2
Suspicious: 0             Time: 2:22
Disinfected: 0
Deleted: 0                Press any key to continue.
Renamed: 0

Time: 2:22
                                                                   ESC-Cancel
```

Results of Virus Scanning

Search

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



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

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

                         ENTER-Select  ESC-Cancel

Search on local hard disks.
```

Scan Search Menu

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

Local Hard Disks

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

Diskette Drive A:

This option scans floppy disks in drive A for viruses.

Network Drives

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

CD-ROM Drives

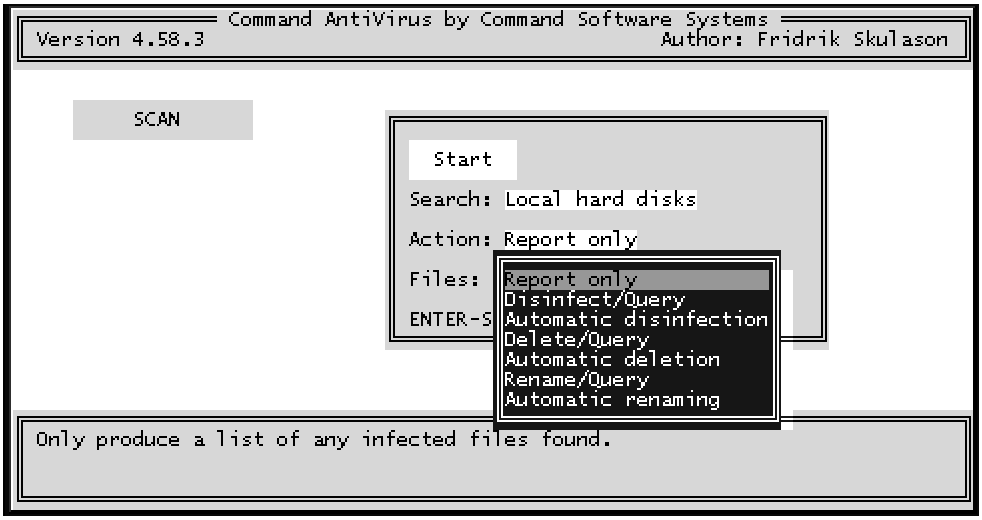
This option scans CDs.

User-Specified

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

Action

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



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

SCAN

Start
Search: Local hard disks
Action: Report only
Files:
ENTER-S

Report only
Disinfect/Query
Automatic disinfection
Delete/Query
Automatic deletion
Rename/Query
Automatic renaming

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

Scan Action Menu

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

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

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

Report Only

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

Disinfect/Query

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

Automatic Disinfection

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

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

Delete / Query

This option prompts you before deleting an infected file.

Automatic Deletion

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

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

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

Rename/Query

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

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

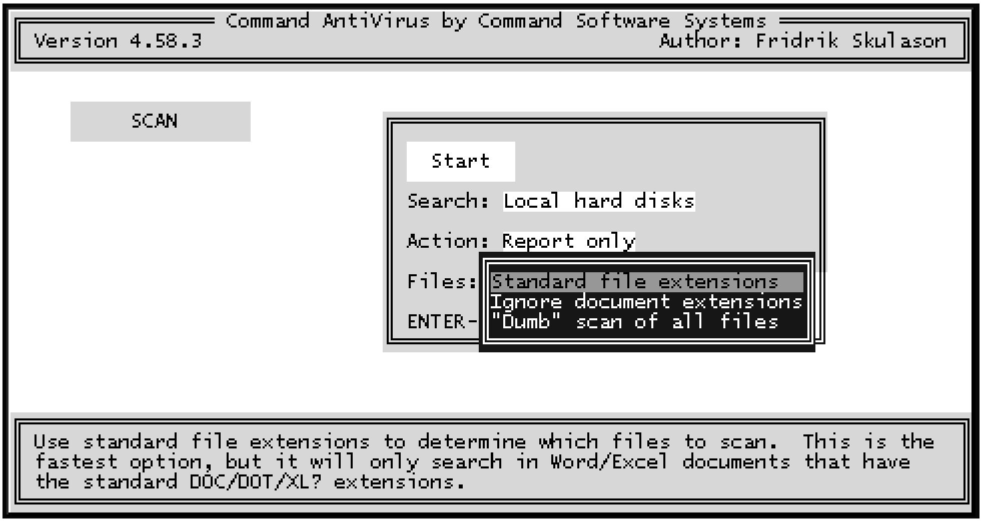
Use this option if you want study the infected file or compare it to a virus-free backup copy.

Automatic Renaming

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

Files

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



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

    SCAN                    Start

                            Search: Local hard disks

                            Action: Report only

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

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

Scan Files Menu

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

Standard File Extensions

These are the file types that are normally targeted by viruses for infection. To provide the most up-to-date 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.

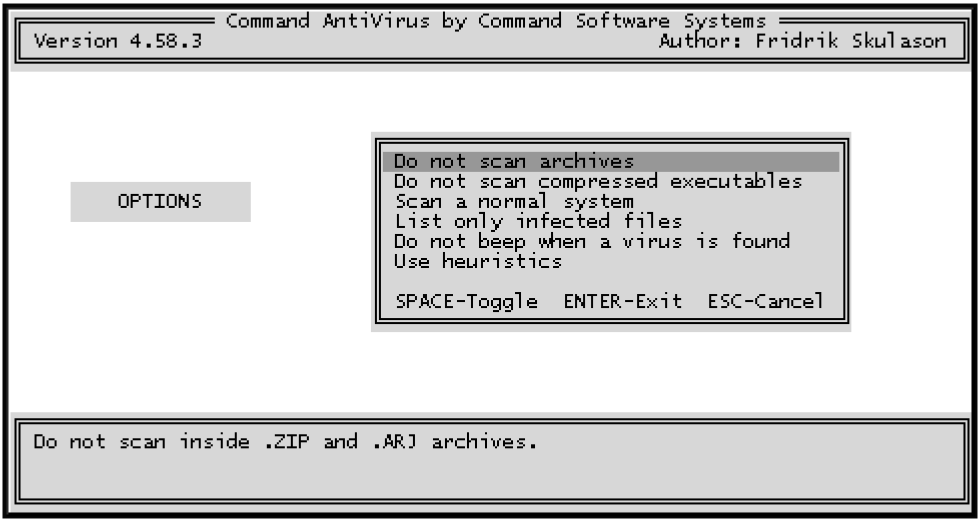
“Dumb” Scan of All Files

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:



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

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

                          SPACE-Toggle  ENTER-Exit  ESC-Cancel

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

Options Menu

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

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

Do Not Scan Archives

This option does not scan inside archives.

Do Not Scan Compressed Executables

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

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

Scan a Normal System

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

List Only Infected Files

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

Do Not Beep When a Virus Is Found

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

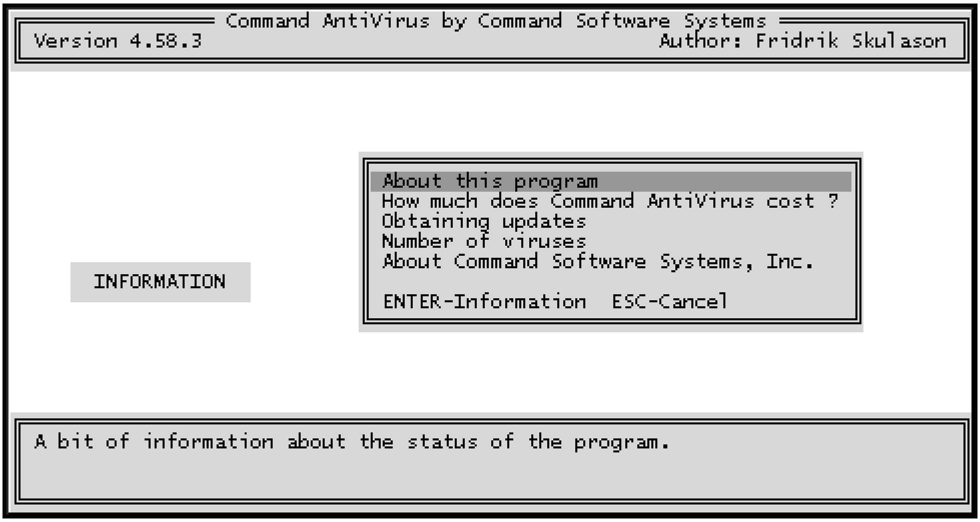
Use Heuristics

This option allows you to select the heuristics scanning method.

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

INFORMATION

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



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

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

                                ENTER-Information  ESC-Cancel

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

Information Menu

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

About This Program

This option provides information about the status of the program.

How Much Does Command AntiVirus Cost?

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

Obtaining Updates

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

Number of Viruses

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

About Command Software Systems, Inc.

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

QUIT

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

COMMAND-LINE MODE

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

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

Switch	Description
/APPEND	Appends a new report to an existing one. Use this with the /REPORT switch.
/ARCHIVE	Scans inside archives.
/AUTO	Use with /DELETE or /DISINF switch so that Command AntiVirus will not prompt you before deleting or disinfecting a file. When used without /AUTO, /DELETE and /DISINF prompt you before taking any action.
/BEEP	Generates a beep when a virus is found.
/COLLECT	Scans for a virus collection.
/DELETE	Deletes all infected files. We do not recommend using this switch as some viruses encrypt portions of the drive.
/DISINF	Disinfects whenever possible. This option deletes some overwriting and first-generation virus samples. A first-generation virus is the “starter” program that begins the infection process. Encountering a first generation virus is very rare. This option will never delete a file that CSAV can disinfect.
/DUMB	Scans **all** files. **Caution**: We do **not** recommend this option for inexperienced users as scanning all files on a disk could produce a false indication of a virus infection.
/FREEZE	Halts the computer when the program finds a virus.
/HARD	Scans all the physical hard drives in the system.
/HELP or /?	Displays a list of available options.
/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 ***Network Administration*** chapter.
/NOFILE	Does **not** scan for file viruses.
/NOFLOPPY	This switch is for use on a system without floppy drives.
/NOHEUR	Disables heuristics.
/NOMEM	Does **not** scan memory for viruses.
/NOSUB	Does **not** scan subdirectories.
/PACKED	Unpacks compressed executables.
/PAGE	Pauses after every screen while displaying a report.
/REMOVEALL	Removes all macros from all documents.
/REMOVENEW	Removes new variants of macro viruses by removing all macros from infected documents.
/RENAME	Renames infected COM/EXE files to VOM/VXE. You can use this switch with /AUTO.
/REPORT=	Sends the output to the file you specify to the right of the equals (=) sign.
/SAFEREMOVE	Removes all macros from documents if a known virus is detected.
/SILENT	Generates **no** screen output at all. This is useful when running F-PROT.EXE from a batch file where you will check for return codes.
/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.

6

NETWORK ADMINISTRATION

This chapter contains information on what administrators need to do to prepare for the installation of Command AntiVirus for Windows® Version 4.70 or higher across the network. It outlines the steps that you need to take to customize, install, update, and upgrade Command AntiVirus for Windows quickly and easily.

The administrative tools provided in our centralized management package called COMMANDCentral will help you to accomplish these tasks.

COMMANDCentral allows administrators to prepare the Command AntiVirus installation for deployment and schedule downloads of Command AntiVirus updates and upgrades. It contains the following tools:

- Command AntiVirus Deployment Prep Wizard
- System Policy Template for Windows Installer
- System Policy Template for Command AntiVirus
- Custom Installation Wizard for Command AntiVirus
- Command AntiVirus Download Manager

For more information on these tools, refer to the ***COMMANDCentral*** chapter of this guide.

PREPARING FOR THE INSTALLATION

Before you can deploy Command AntiVirus across your network, there are several steps that you must take to prepare for the installation.

These steps include:

1. **Taking an inventory of the platforms that are supported on your network**

   For example, does the network consist of machines running Windows 2000, Windows XP, Windows NT®, Windows 95/98/Me, or a combination of these platforms?

2. **Deciding on a prerequisite distribution point**

   95/98/Me

   For networks containing **only** Windows 95/98/Me machines, you **must** use the prerequisite component files located in the **COMMANDCentral** folder.

   Windows 95/98/Me and Windows NT machines require that certain prerequisite component files be installed prior to the installation of CSAV. The Command AntiVirus Deployment Prep Wizard allows you to prepare your machines from an NTFS shared drive on a server.

3. **Deciding where to create an administrative image**

   Updating and upgrading CSAV is much easier if you perform an administrative installation to a shared network folder. The shared network folder is called the Software Distribution Point (SDP), and the files in the folder are called the administrative image. You can create as many administrative images and SDPs as you need.

4. **Deciding which deployment method(s) to use**

   Several options are available to customize and install CSAV across your network. Your inventory of platforms will help you decide which method(s) to use.

Your options include:

- Using the Command AntiVirus Deployment Prep Wizard RunP
- Using the Custom Installation Wizard for Command AntiVirus **MSIEXEC**
- Using System Policy
- Using Active Directory
- Using a combination of these methods

For more information, refer to **Selecting a Deployment Method** located later in this chapter.

5. Preparing selected machines

If you are preparing machines on a network that contains **only** Windows 95/98/Me machines, refer to **Starting The Installation Process** located later in this chapter.

Using the Command AntiVirus Deployment Prep Wizard, you can create a prerequisite distribution point and select the Windows NT machines that you want to prepare with the prerequisite component files.

NOTE: You do **not** need to select Windows 95/98/Me machines.

For more information on the Command AntiVirus Deployment Prep Wizard, refer to **Preparing For Deployment** located in the ***COMMANDCentral*** chapter of this guide.

6. Creating an administrative image

There are three ways to create an administrative image. Your method of deployment and the tasks that you are performing will help you decide which method to use. For more information, refer to **Installing Command AntiVirus to a Software Distribution Point (SDP)** located later in this chapter.

7. Customizing Command AntiVirus

There are two ways to customize Command AntiVirus before deploying CSAV across your network. Your method of deployment and the items that you want to customize will help you decide which method to use. For more information, refer to **Customizing Command AntiVirus** located later in this chapter.

8. Advertising Command AntiVirus across your network

95/98/Me

If you are deploying to Windows 95/98/Me machines, you do **not** need to advertise or install with elevated privileges.

Before you can install CSAV on machines running Windows 2000, Windows XP, and Windows NT, you need to apply administrative rights to install (advertise) to the CSAV installation package.

How you do this depends on which method you are using to deploy CSAV. For more information, refer to **Advertising Command AntiVirus** located later in this chapter.

NT

If you are using System Policy to deploy to Windows NT machines, you do **not** need to advertise CSAV. Instead, you need to customize the Windows Installer to install with elevated privileges. This action only allows the user to install software. It does **not** give the user additional rights. For more information, refer to **Selecting A Deployment Method** located later in this chapter.

9. Starting the installation process

There are four ways to install CSAV across your network. Your inventory of machines and your method of deployment determine which method to use. For more information, refer to **Starting the Installation Process** located later in this chapter.

RECOMMENDED METHODS FOR MULTI-PLATFORM NETWORKS

If your network consists of machines running several different Windows 32-bit platforms, we recommend using the following method to prepare, customize, and install Command AntiVirus across your network.

Using the Command AntiVirus Deployment Prep Wizard:

1. Specify a Prerequisite Distribution Point
2. Create an administrative image or specify the location of the administrative image

NOTE: You can also create an administrative image from a downloaded version of Command AntiVirus using the Command AntiVirus Download Manager. You can then specify the location of the administrative image in the Command AntiVirus Deployment Prep Wizard.

If you want to create an installation SDP on multiple servers, we recommend that you use the Command AntiVirus Download Manager to create an administrative image. For more information, refer to **Command AntiVirus Download Manager** located in the ***COMMANDCentral*** chapter of this guide.

3. Customize Command AntiVirus by creating an MST
4. Select and prepare Windows NT machines for installation

You can prepare Windows 95/98/Me machines by placing the **CSS Remote Agent RunP** that is created by the wizard in a logon script, web page, Microsoft® SMS script, or Novell® ZENworks®. For more information, refer to **Starting The Installation Process** located in later in this chapter

5. Advertise Command AntiVirus
6. Start the installation process by running the Command AntiVirus Deployment Prep Wizard **RunP** command line. For more information, refer to **Starting The Installation Process** located later in this chapter.

For more information on the Command AntiVirus Deployment Prep Wizard, refer to **Preparing for Deployment** in the ***COMMANDCentral*** chapter of this guide.

RECOMMENDED METHODS FOR 9X ONLY NETWORKS

For networks containing machines running **only** Windows 95/98/Me, we recommend the following methods to prepare, customize, and install Command AntiVirus across your network.

1. Configure the Command AntiVirus Download Manager to download the latest version of Command AntiVirus. For more information, refer to **Command AntiVirus Download Manager** located in the ***COMMANDCentral*** chapter of this guide.
2. When the download is complete, use the Command AntiVirus Download Manager to create an administrative image. For more information, refer to **Command AntiVirus Download Manager** located in the ***COMMANDCentral*** chapter of this guide.
3. Using the Custom Installation Wizard for Command AntiVirus from the COMMANDCentral start menu, create an .MST. For more information, refer to **Custom Installation Wizard** located in the ***COMMANDCentral*** chapter of this guide.
4. Using the **CSS Remote Agent RunP** command in a logon script, web page, Microsoft® SMS script, or Novell® ZENworks®, prepare the machines with the prerequisite files. For more information, refer to **Starting The Installation Process** located later in this chapter.
5. Using the Custom Installation Wizard **MSIEXEC** command in a logon script, web page, Microsoft® SMS script, or Novell® ZENworks®, start the installation process. For more information, refer to **Starting The Installation Process** located later in this chapter.

INSTALLING COMMAND ANTIVIRUS TO A SOFTWARE DISTRIBUTION POINT (SDP)

Updating and upgrading Command AntiVirus for Windows is much easier if you perform an administrative installation to a shared network folder. The shared network folder is called the Software Distribution Point (SDP), and the files in the folder are called the administrative image. For example, the administrative image allows you to apply and distribute future patches such as updates to our virus definition files quickly and easily.

You can create as many administrative images and SDPs as you need. Multiple SDPs ensure that there is always a backup copy when an installation needs to be repaired. You can then list these SDPs when you customize your installation settings using the Custom Installation Wizard for Command AntiVirus.

NOTE: Command AntiVirus can **only** be installed from the location from which it was advertised. These additional administrative images for installation provide only a backup copy when an installation needs to be repaired.

For information on creating multiple SDPs from which you can advertise Command AntiVirus, refer to **Creating an Administrative Image of a Downloaded Upgrade** located in the ***COMMANDCentral*** chapter of this guide.

You can create an administrative image:

- Using the Command AntiVirus Deployment Prep Wizard. For information on this wizard, refer to **Preparing For Deployment** located in the ***COMMANDCentral*** chapter of this guide.

NOTE: This option is **not** available for networks containing only Windows 95/98/Me machines.

- From the command line

  At the command line, type the following and press **Enter**.

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

- Using the Command AntiVirus Download Manager. This tool allows you to create an administrative image of downloaded Command AntiVirus updates and upgrades. For more information, refer to **Command AntiVirus Download Manager** located in the ***COMMANDCentral*** chapter of this guide.

NT/2K/XP

- In Windows NT and Windows 2000/XP, this option allows you to create an installation SDP on multiple servers.

SELECTING A DEPLOYMENT METHOD

You have several options in deploying Command AntiVirus for Windows across your network. Your inventory of platforms and the tools you use to administer your network will help you decide which method or methods to use.

These options include:

- Using the Command AntiVirus Deployment Prep Wizard RunP
- Using the Custom Installation Wizard for Command AntiVirus **MSIEXEC**
- Using System Policy
- Using Active Directory
- Using a combination of these methods

USING THE CSAV DEPLOYMENT PREP WIZARD RUNP

95/98/Me

For networks containing **only** Windows 95/98/Me machines, refer to **Using the Custom Installation Wizard MSIEXEC** located later in this section.

You can use this method to deploy Windows 95/98/Me machines, Windows NT machines and/or Windows 2000 and Windows XP machines that do not have Active Directory installed.

The Command AntiVirus Deployment Prep Wizard allows you to prepare machines for installation, create an administrative image, customize CSAV, and advertise CSAV across your network.

It also provides you with a **RunP** command line that you can put in a logon script, web page, Microsoft® SMS script, or Novell® ZENworks® to start the installation of CSAV onto machines across your network.

95/98/Me

For networks containing **only** Windows 95/98/Me machines, use the **MSIEXEC** command line that is created when you create a customized MST using this wizard.

For more information, refer to **Starting the Installation Process** located later in this chapter.

USING THE CUSTOM INSTALLATION WIZARD MSIEXEC

Although you can use this method to deploy Command AntiVirus on any Windows 32-bit platform, we recommend this method for networks containing machines running **only** Windows 95/98/Me.

When you use the Custom Installation Wizard to customize Command AntiVirus, the wizard creates an MSIEC command line. You can put this command line in a logon script, web page, Microsoft® SMS script, or Novell® ZENworks® to start the installation of CSAV onto machines across your network.

95/98/Me

For networks containing **only** Windows 95/98/Me machines, use the **MSIEXEC** command line that is created when you create a customized MST using the Custom Installation Wizard for Command AntiVirus from the COMMANDCentral **Start** menu.

For more information, refer to **Starting the Installation Process** located later in this chapter.

USING SYSTEM POLICY

9x/Me/NT

You can use this method to deploy Windows 95/98/Me and Windows NT machines.

95/98/Me

To use this method on Windows 95/98/Me machines, you **must** have a network client installed on the machines.

After you have prepared your machines for installation, created an administrative image, and customized CSAV, you can then start the installation of CSAV onto machines across your network. You can do this using e-mail, a logon script, web page, Microsoft SMS script, or Novell ZENworks.

NOTE: On machines running Windows NT, as the Command AntiVirus installation requires that you are a member of the administrator's group on the local machine, you must first customize the Windows Installer to install with elevated privileges. This action only allows the user to install software. It does **not** give the user additional rights.

For more information on customizing the Windows Installer, refer to **System Policy Template for Windows Installer** located in the ***COMMANDCentral*** chapter of this guide.

When you set the Windows Installer to install with elevated privileges, this setting applies to **all** applications not just to Command AntiVirus.

For more information, refer to **Starting the Installation Process** located later in this chapter.

USING ACTIVE DIRECTORY

2K/XP

You can use this method to deploy Windows 2000 and Windows XP machines that have Active Directory installed.

After you have created an administrative image and customized CSAV, you can then start the installation of CSAV onto machines across your network. You can do this by assigning applications to computers using Group Policy.

For more information, refer to **Starting the Installation Process** located later in this chapter.

USING A COMBINATION OF METHODS

Depending on your inventory of platforms and the tools you use to administer your network, you may want to use a combination of these methods.

For example, let’s say that your network is made up of machines running Windows NT and Windows 2000 and Windows XP with Active Directory installed. You may want to use the Command AntiVirus Deployment Prep Wizard or System Policy to deploy the Windows NT machines. You can then use Active Directory to deploy the Windows 2000 and Windows XP machines.

CUSTOMIZING COMMAND ANTIVIRUS

COMMANDCentral comes with two tools that allow administrators to customize Command AntiVirus before installing over the network onto multiple computers. Determining the method of deployment that you want to use and the installation features and settings that you want to change will help you decide which tool to use.

To customize Command AntiVirus, you can use either of the following tools:

- **Custom Installation Wizard for Command AntiVirus** – Allows you to configure installation features, settings for the items on the Command AntiVirus **Preferences** menu, and scan tasks. You can also import settings from a previous version of Command AntiVirus and identify additional Software Distribution Points (SDPs).

  The wizard uses the Command AntiVirus Windows Installer package (MSI) file to create a custom Windows Installer transform (MST file). The MST file contains your customized installation features and settings. For more information, refer to **Customizing Your CSAV Installation Settings** located in the ***COMMANDCentral*** chapter of this guide.

The Custom Installation Wizard for Command AntiVirus is also part of the Command AntiVirus Deployment Prep Wizard.

If you are using an MST file to customize CSAV and are using the Command AntiVirus Deployment Prep Wizard to advertise, you **must** also use the Command AntiVirus Deployment Prep Wizard to create the MST.

For networks containing **only** Windows 95/98/Me machines, you **must** use the Custom Installation Wizard for Command AntiVirus from the COMMANDCentral **Start** menu.

- **System Policy Template for Command AntiVirus** – Allows you to add the template to Group Policy in Windows 2000 and Windows XP or System Policy in Windows 95/98/Me and Windows NT. You can then open the template to configure the installation settings for the items on the Command AntiVirus **Preferences** menu. For more information, refer to **Customizing Your CSAV Installation Settings** located in the ***COMMANDCentral*** chapter of this guide.

NOTE: Using the System Policy Template for Command AntiVirus also allows you to customize your **Preferences** after you have installed CSAV. The changes occur the next time the machine is started.

ADVERTISING COMMAND ANTIVIRUS

95/98/Me

If you are deploying to Windows 95/98/Me machines, you do **not** need to advertise or install with elevated privileges.

To install Command AntiVirus for Windows on machines running Windows NT, Windows 2000, and Windows XP, you must be signed on as a member of the administrator's group on the local machine. Therefore, if you are using Active Directory or the Command AntiVirus Deployment Prep Wizard **RunP** command line to deploy CSAV, you must first apply administrative rights to install (advertise) to the CSAV installation package. How you do this depends on which method you use to deploy.

CSAV DEPLOYMENT PREP WIZARD RUNP

If you are deploying to machines running Windows NT and/or Windows 2000 and Windows XP that do not have Active Directory installed, you can use the Command AntiVirus Deployment Prep Wizard to advertise Command AntiVirus. For more information, refer to **Preparing For Deployment** located in the ***COMMANDCentral*** chapter of this guide.

ACTIVE DIRECTORY

2K/XP

If you are deploying to machines running Windows 2000 and Windows XP with Active Directory installed, you can use Group Policy to assign the installation package to computers. For more information, refer to **Starting the Installation Process** located later in this chapter.

STARTING THE INSTALLATION PROCESS

There are four ways to start the installation of CSAV across your network. This section contains information on each method.

- Using the Command AntiVirus Deployment Prep Wizard RunP
- Using the Custom Installation Wizard for Command AntiVirus **MSIEXEC**
- Using System Policy
- Using Active Directory

USING THE CSAV DEPLOYMENT PREP WIZARD RUNP

For networks containing **only** Windows 95/98/Me machines, refer to **Using the Custom Installation Wizard MSIEXEC** located later in this section.

After you have created an administrative image and advertised CSAV using the Command AntiVirus Deployment Prep Wizard, you can then install CSAV across your network using the Command AntiVirus Deployment Prep Wizard **RunP** command line.

NOTE: You must run the **RunP** command line from each machine on which you want to install CSAV.

Just copy and paste the **RunP** command line from the **Install to Network** dialog box into a logon script, web page, Microsoft SMS script, or Novell ZENworks. CSAV installs the next time the computer is started.

As the installation of the prerequisite component files requires the machine to be restarted, it may require a second startup before the installation begins.

For Windows 95/98/Me machines, as the installation of the prerequisite component files does **not** start automatically, you **must** place the **CSS Remote Agent RunP** that is created by the wizard into a logon script, web page, Microsoft SMS script, or Novell ZENworks.

The wizard creates the **CSS Remote Agent RunP** in the **CSS_PCM** folder on the server and NTFS drive that you specified in the wizard. You can use the same logon script that you use for the installation **RunP**, but the **CSS Remote Agent RunP** should be placed before the installation **RunP** in the logon script.

If you are using an e-mail to start the installation of the prerequisite files, do **not** send out the **RUNP.EXE** file. As the **RUNP.EXE** uses other files, send **only** a link to the **RUNP.EX**E.

USING THE CUSTOM INSTALLATION WIZARD MSIEXEC

We recommend using this method for networks containing **only** Windows 95/98/Me machines.

After you have created an administrative image, you can then install Command AntiVirus across your network using the **MSIEXEC** command line. This command line is created when you create a customized MST using the Custom Installation Wizard for Command AntiVirus.

For networks containing **only** Windows 95/98/Me machines, you **must** use the Custom Installation Wizard for Command AntiVirus from the COMMANDCentral **Start** menu.

Just copy and paste the **MSIEXEC** command line from the **Finished** dialog box into a logon script, web page, Microsoft SMS script, or Novell ZENworks. CSAV installs the next time the computer is started.

For Windows 95/98/Me machines, you **must** add a path of **C:\WINDOWS\SYSTEM** to the command line for the command to run:

```
C:\Windows\System\msiec.exe/I\\server\shared\csav.msi
Transforms=\\server\shared\custom.mst
```

NOTE: You must run the **MSIEXEC** command line from each machine on which you want to install CSAV.

For Windows 95/98/Me machines, as the installation of the prerequisite component files does **not** start automatically, you **must** place the **CSS Remote Agent RunP** located in **C:\Program Files\Command Software\CommandCentral** into a logon script, web page, Microsoft SMS script, or Novell ZENworks.

You can use the same logon script that you use for the installation **MSIEXEC,** but the **CSS Remote Agent RunP** should be placed before the installation **msiexec** in the logon script.

If you are using an e-mail to start the installation of the prerequisite files, do **not** send out the **RUNP.EXE** file. As the **RUNP.EXE** uses other files, send **only** a link to the **RUNP.EX**E.

As the installation of the prerequisite component files requires the machine to be restarted, it may require a second startup before the installation begins.

USING SYSTEM POLICY

After you have created an administrative image, customized CSAV, and customized the Windows Installer to install with elevated privileges, you can then install CSAV across your network using e-mail, a logon script, web page, Microsoft SMS script, or Novell ZENworks. CSAV installs the next time the computer is started.

NOTE: You must run this command line from each machine on which you want to install CSAV.

USING ACTIVE DIRECTORY

You can use Group Policy on computers running Windows 2000 or Windows XP with Active Directory installed to deploy Command AntiVirus for Windows to individual computers from a central location on a network. This section provides information on:

- Configuring group policies for Command AntiVirus
- Assigning the installation package to computers
- Deploying updated Command AntiVirus definition files
- Deploying new versions of Command AntiVirus
- Removing Command AntiVirus for Windows

Getting Started

Consider the following Microsoft requirements before proceeding with the steps that are described in this section. For more information about Group Policy, refer to the documentation that came with your Windows 2000 or Windows XP operating system software.

- To set Group Policy or Software Installation snap-ins for a domain, you must use a computer that is configured as a domain controller.
- To set policies for an organizational unit in a domain, you must be an administrator for that domain or have equivalent rights.

Group Policy-based deployment simplifies software installation and maintenance of assigned applications. Using Windows 2000 or Windows XP Group Policy, you can distribute Command AntiVirus for Windows by **Assigning applications to computers**. Through this assignment, CSAV installs the next time the computer is started.

Configuring Group Policies

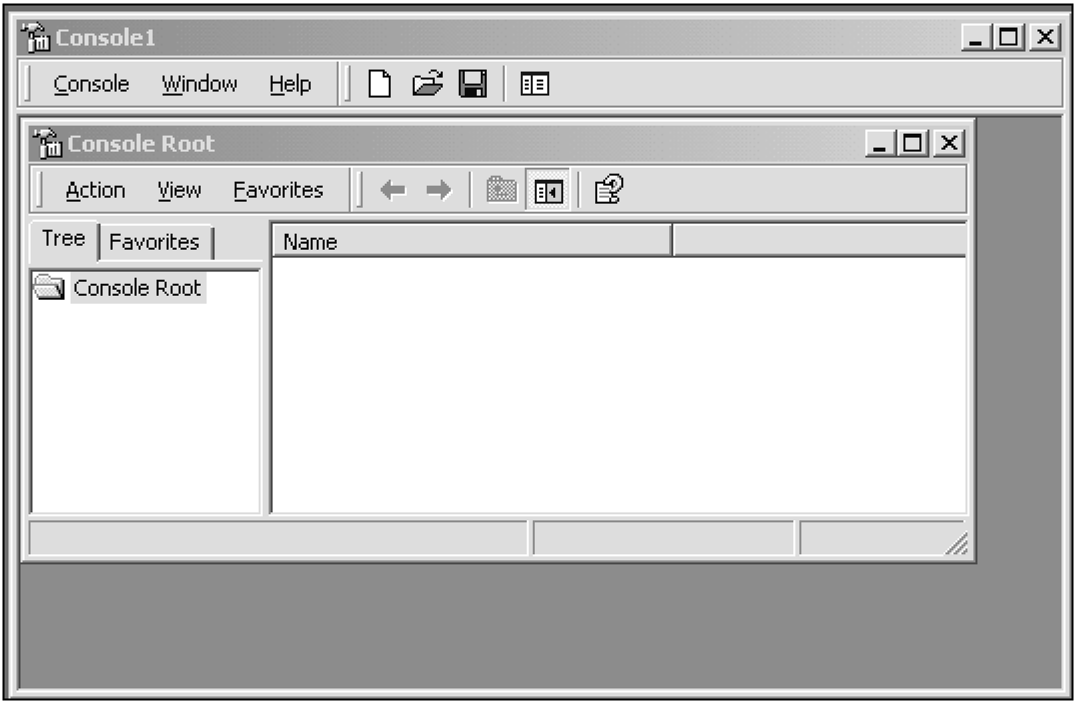
Before you can install Command AntiVirus for Windows onto individual computers from a central location on a network, you must open the Software Installation snap-in and create a Group Policy object for the group of users, computers, or domains (including domain servers) that you want to target during deployment. You can then save your selections for future use by creating a Microsoft Management Console (MSC file). The following information will help you through this process.

NOTE: For more information on installing Command AntiVirus for Windows to a central location on a network, refer to **Installing Command AntiVirus to a Software Distribution point (SDP)** located previously in this chapter.

To configure group policies for Command AntiVirus for Windows, follow these steps:

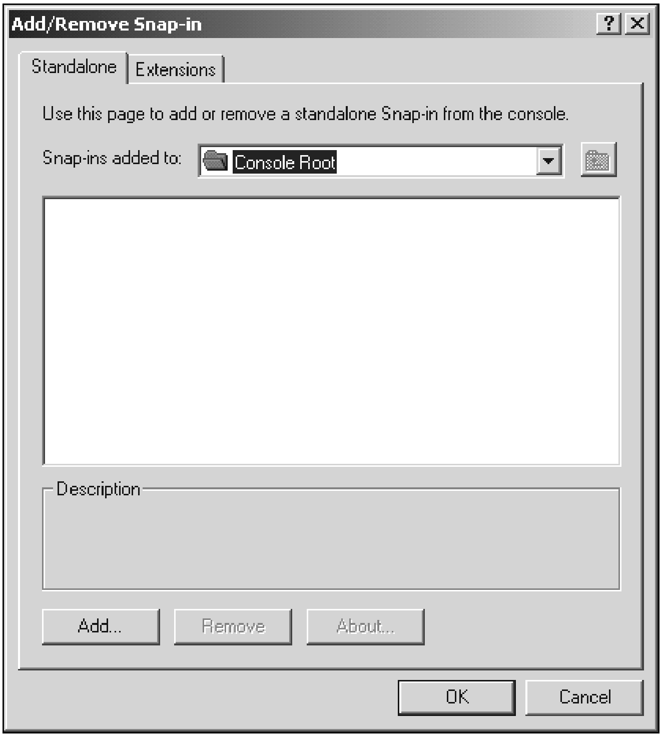
1. Click the **Start** button on the Windows task bar.
2. Click **Run**.
3. In the text box, type **mmc**.

4. Click **OK**. The system displays the **Microsoft Management Console**:



Microsoft Management Console

5. From the **Console** drop-down menu, select **Add/Remove Snap-in...**. The system displays the **Add/Remove Snap-in** dialog box:

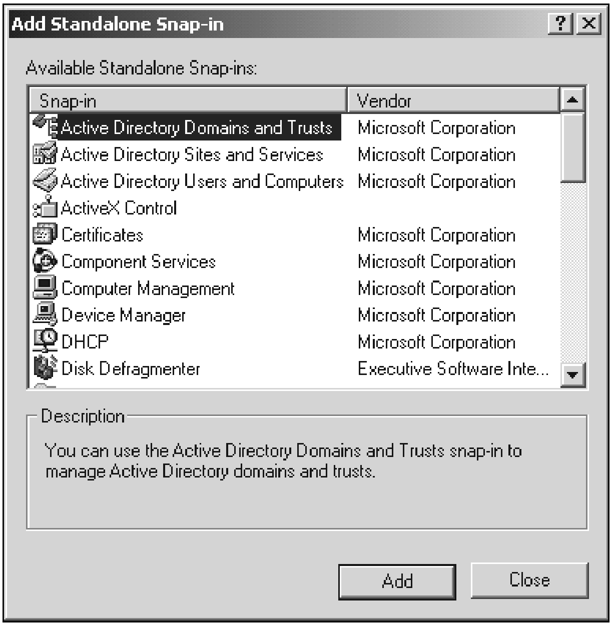

Add/Remove Snap-in

Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Add/Remove Snap-in Dialog Box

6. Click **Add**. The system displays the **Add Standalone Snap-in** dialog box:



Add Standalone Snap-in

Available Standalone Snap-ins:

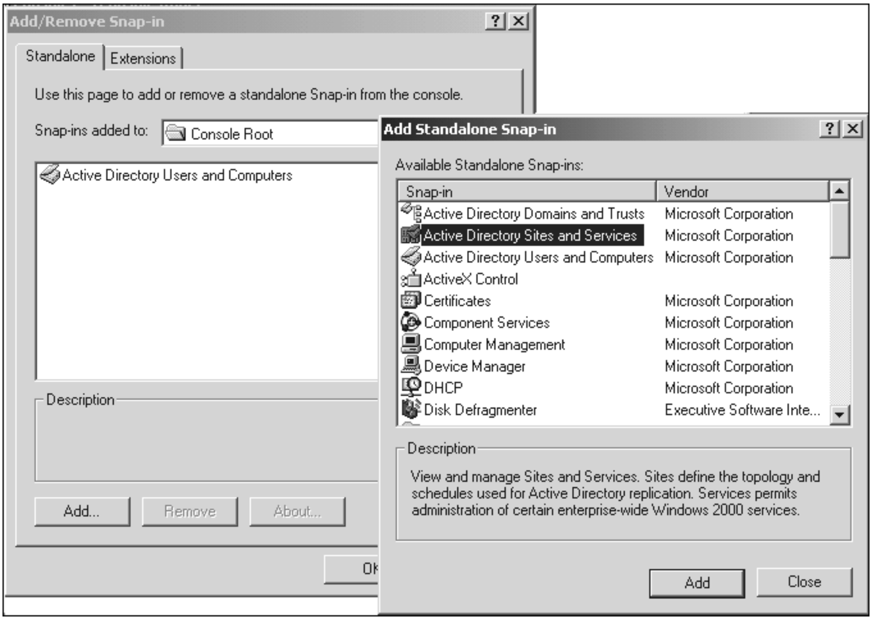
Snap-in	Vendor
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Computers	Microsoft Corporation
ActiveX Control	
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
DHCP	Microsoft Corporation
Disk Defragmenter	Executive Software Inte...

Description

You can use the Active Directory Domains and Trusts snap-in to manage Active Directory domains and trusts.

Add Standalone Snap-in Dialog Box

7. From the **Add Standalone Snap-in** list, select **Active Directory Users and Computers** and click **Add.** This item is now added to the **Add/Remove Snap-in** list:



Add/Remove Snap-in

Standalone | Extensions

Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

Active Directory Users and Computers

Description

Add... Remove About...

OK

Add Standalone Snap-in

Available Standalone Snap-ins:

Snap-in	Vendor
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Computers	Microsoft Corporation
ActiveX Control	
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
DHCP	Microsoft Corporation
Disk Defragmenter	Executive Software Inte...

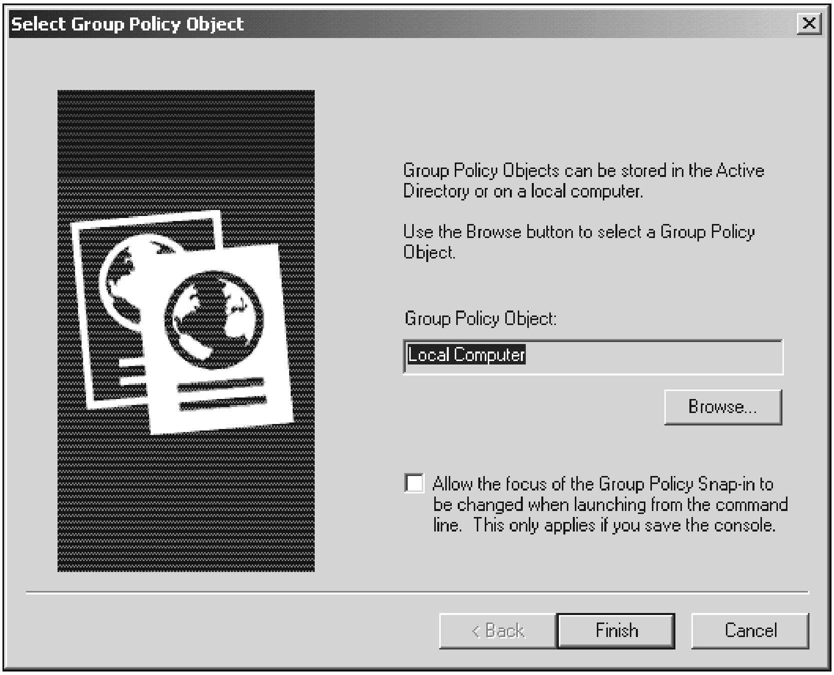
Description

View and manage Sites and Services. Sites define the topology and schedules used for Active Directory replication. Services permits administration of certain enterprise-wide Windows 2000 services.

Add Close

Add/Remove Snap-in Dialog Box and Add Standalone Snap-in List

8. From the **Add Standalone Snap-in** list, select **Active Directory Sites and Services** and click **Add**. This item is now added to the **Add/Remove Snap-in** list.
9. From the **Add Standalone Snap-in** list, select **Group Policy** and click **Add**. The system displays the **Select Group Policy Object** dialog box:



Select Group Policy Object

Group Policy Objects can be stored in the Active Directory or on a local computer.

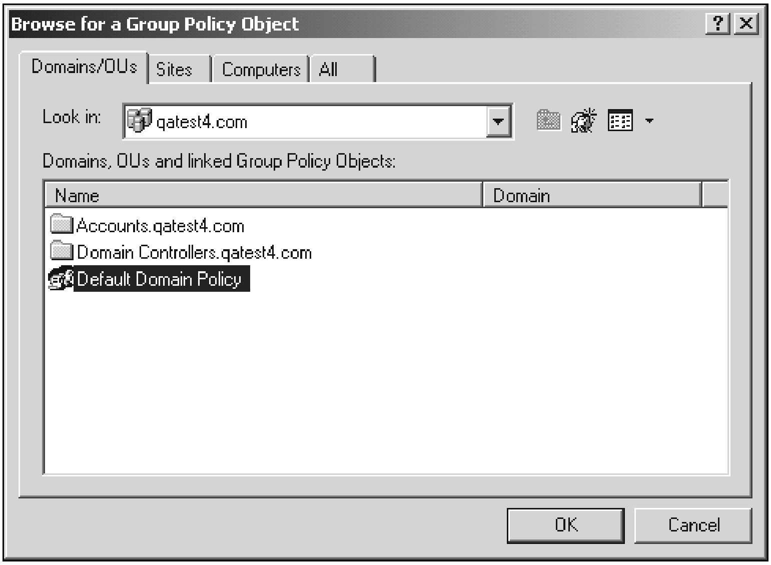
Use the Browse button to select a Group Policy Object.

Group Policy Object: Local Computer

□ Allow the focus of the Group Policy Snap-in to be changed when launching from the command line. This only applies if you save the console.

Select Group Policy Object Dialog Box

10. Click **Browse** to select a Group Policy object. The system displays the **Browse for a Group Policy Object** dialog box:



Browse for a Group Policy Object
Domains/OUs
Sites
Computers
All
Look in:
qatest4.com
Domains, OUs and linked Group Policy Objects:
Name
Domain
Accounts.qatest4.com
Domain Controllers.qatest4.com
Default Domain Policy
OK
Cancel

Browse Group Policy Object Dialog Box

11. From the **Domains/OUs**, **Sites**, **Computers**, or **All** tab, select the Group Policy object for the group of users, computers, or domains (including domain servers) that you want to target during deployment.

    If you need to create a new Group Policy object for your selected group, right-click in the list box. The system displays a drop-down menu. Click **New.** Then, in the text box that is now in the **Name** list, type the name of the new Group Policy object and press **Enter**.

12. Click **OK**. The system returns to the **Select Group Policy Object** dialog box.

13. Click **Finish** to add your group policy to the **Add/Remove Snap-in** list. The system returns to the **Add Standalone Snap-in** dialog box.

    Repeat **Steps 9** through **13** to add additional group policies.

14. In the **Add Standalone Snap-in** dialog box, click **Close**.

15. In the **Add/Remove Snap-in** dialog box, click **OK**. The system returns to the **Microsoft Management Console**.
16. From the **Console** drop-down menu, select **Save As**. The system displays the **Save As** dialog box.
17. Type a name in the File name text box, for example:

    ```
    CSAVConsole.msc
    ```

18. Click **Save**.

    You are ready to assign Command AntiVirus for Windows to individual computers.

19. Proceed to **Assigning Command AntiVirus to Computers**.

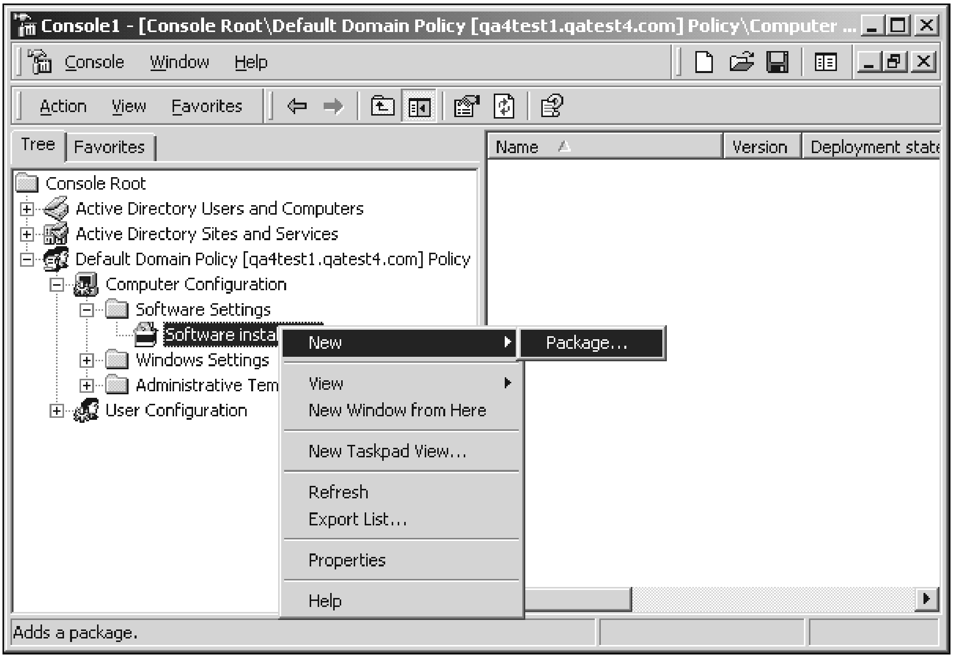
Assigning Command AntiVirus to Computers

Assigning Command AntiVirus for Windows through **Computer Configuration** installs the program when the local computer is started.

NOTE: If you are deploying a custom installation, make sure that you have customized your settings through the Custom Installation Wizard for Command AntiVirus or through the System Policy Template for Command AntiVirus. For more information, refer to **Customizing Command AntiVirus** located previously in this chapter.

To assign Command AntiVirus to computers, follow these steps:

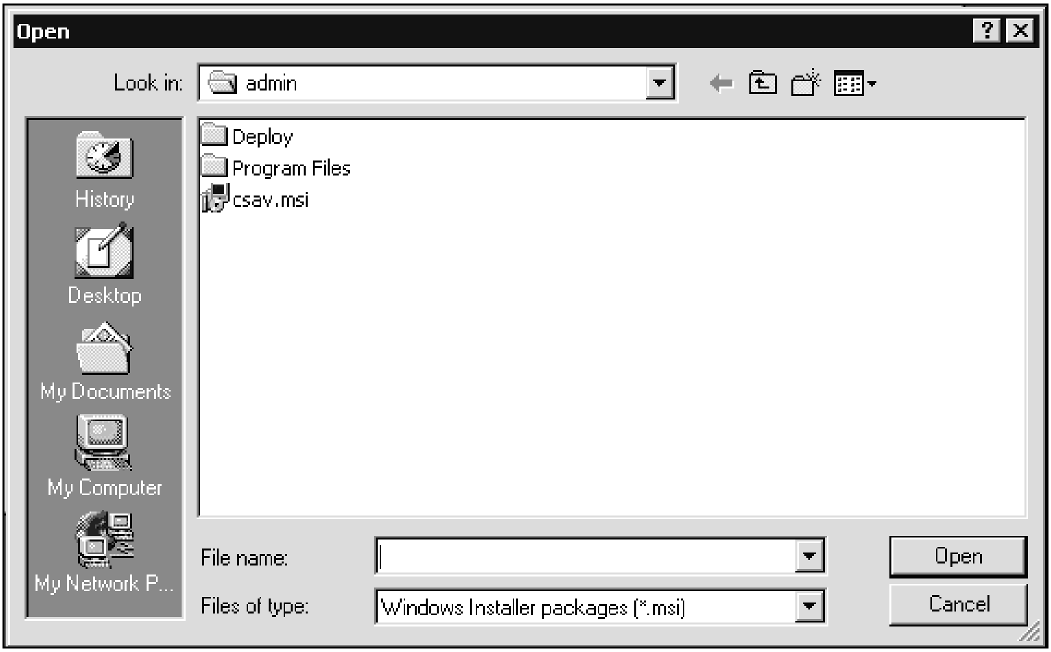
1. In the **Console Root Tree** of the **Microsoft Management Console**, click the plus sign next to the Group Policy object that you selected for Command AntiVirus. This action expands the item. Then, expand **Computer Configuration** and **Software Settings**.
2. Right-click **Software Installation.** The system displays a drop-down menu:



Adds a package.

Software Installation Drop-down Menu

3. Select **New** and click **Package....** The system displays the **Open** dialog box:



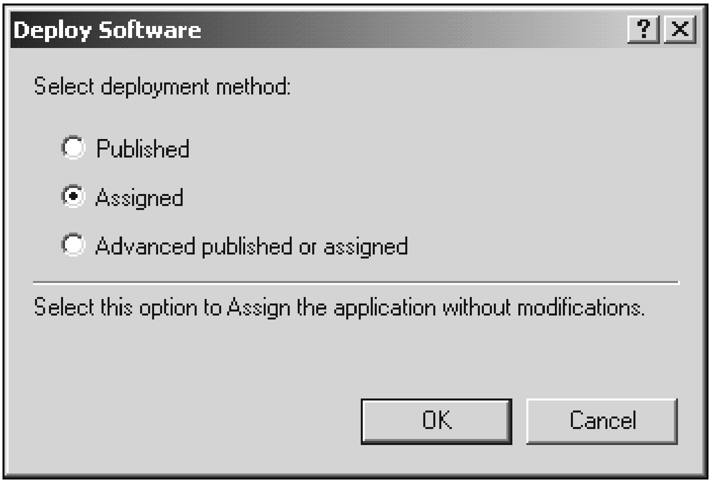
Look in: admin

File name:

Files of type: Windows Installer packages (*.msi)

Open Dialog Box

4. Select the **CSAV.MSI** Windows installer package in the shared network folder, and click **Open**. The system displays the **Deploy Software** dialog box:



Deploy Software

Select deployment method:

○ Published

● Assigned

○ Advanced published or assigned

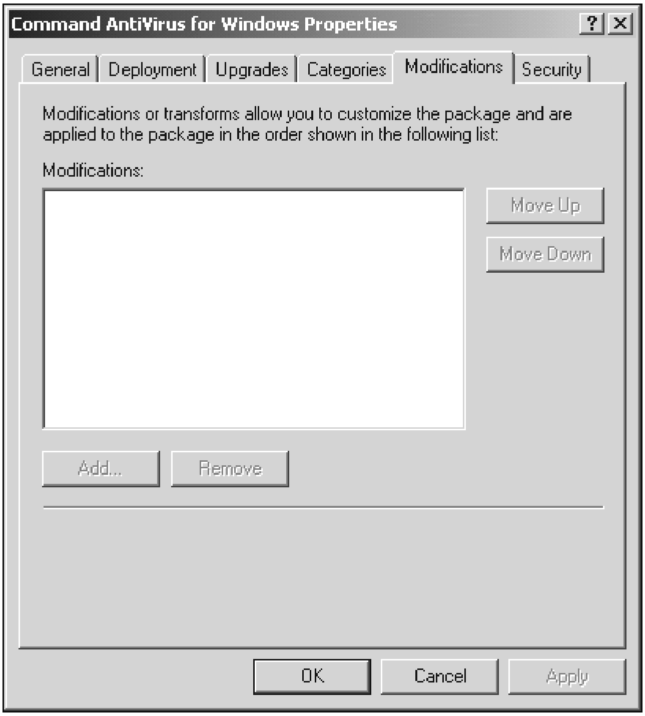
Select this option to Assign the application without modifications.

Deploy Software Dialog Box

5. If you are deploying a **Typical** installation or using the System Policy Template for Command AntiVirus to customize CSAV, select **Assigned** and click **OK**. The system returns to the **Microsoft Management Console**. Your deployment is complete. Command AntiVirus will be installed onto the computers that you selected the next time the computers are started. You have finished this section.

   If you are deploying a **Custom** installation, proceed to **Step 6**.

6. Select **Advanced published or assigned** and click **OK**. The system displays the **Command AntiVirus for Windows Properties** dialog box.
7. Click the **Modifications** tab. The system displays the **Modifications** dialog box:



Command AntiVirus for Windows Properties

Modifications or transforms allow you to customize the package and are applied to the package in the order shown in the following list:

Modifications:

Modifications Dialog Box

8. Click **Add**. The system displays the **Open** dialog box.
9. Select the **CSAV.MST** file in the shared network folder, and click **Open**. The system returns to the **Modifications** dialog box.

Repeat **Steps 8** and **9** for all other MST files that you want to add.

NOTE: Do not click **OK** until you have added all MST files in their proper order. You can use the **Move Up** and **Move Down** buttons to change the order of the files.

10. Click **OK**. The system returns to the **Microsoft Management Console**.

Your deployment is complete. Command AntiVirus will be installed onto the computers that you selected the next time the computers are started.

Updating Deffiles Manually

To provide protection against new viruses, we update the Command AntiVirus definition files (deffiles) frequently.

✓ **NOTE:** You can download updated deffiles, apply the updated patch to the administrative image, and distribute the patch automatically using the Command AntiVirus Download Manager. For more information, refer to **Configuring The Download Process** located in the ***COMMANDCentral*** chapter of this guide.

You can download the file called **DEFMSP.EXE** from the Command Software web site at www.commandsoftware.com. **DEFMSP.EXE** is a self-extracting file that contains the latest deffiles patch (**.MSP**). You can then distribute the patch through Group Policy onto the computers that were specified in the original deployment configuration.

We recommend that you perform an administrative installation of the deffiles patch to your software distribution points (SDPs). This allows you to apply and distribute the patch easily through Group Policy.

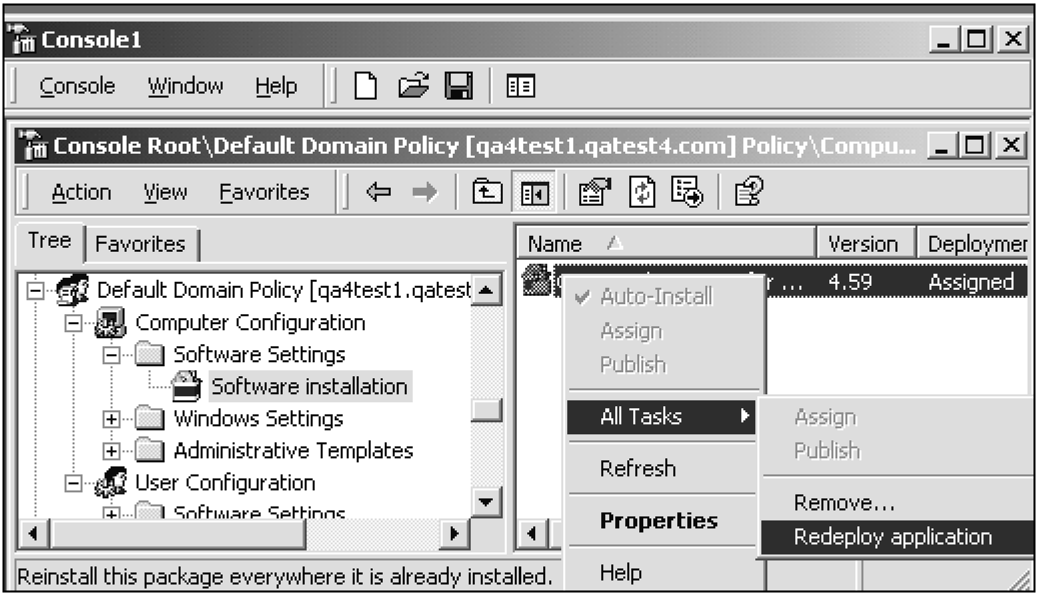
To perform an administrative installation of the deffiles patch, at the command line, type the following and press **Enter**.

```
msiexec /a csav.msi /p csav.msp
```

✓ **NOTE:** Be sure to select the same network path that you used for the original SDP. The name of the CSAV MSP file changes with each update.

To distribute the deffiles patch follow these steps:

1. In the **Console Root Tree** of the **Microsoft Management Console**, click the plus sign next to the Group Policy object that you selected for Command AntiVirus. This action expands this item. Then, expand **Computer Configuration** and **Software Settings**.
2. Click **Software Installation**. The right-hand pane now lists Command AntiVirus.
3. Right-click **Command AntiVirus**. The system displays a drop-down menu:



Reinstall this package everywhere it is already installed.

Package Drop-down Menu – All Tasks

4. Select **All Tasks** and click **Redeploy application**. The system displays a dialog box asking you if you want to continue.
5. Click **Yes**.

Your redeployment is complete. Command AntiVirus with the updated deffiles will be reinstalled onto the computers that were specified in the original deployment configuration the next time the computers are started.

Upgrading Command Antivirus

We recommend that you perform an administrative installation of the Command AntiVirus upgrade package to your software distribution points (SDPs). This allows you to easily apply and distribute the upgrade through Group Policy onto the computers that were specified in the original deployment configuration. For more information, refer to **Installing Command AntiVirus To a Software Distribution point (SDP)** located previously in this chapter.

If you want to customize the installation features and settings of the Command AntiVirus upgrade package, you must create a custom Windows installer transform (MST file) before you install the upgrade. For more information, refer to **Customizing Your Installation Settings** located previously in this chapter.

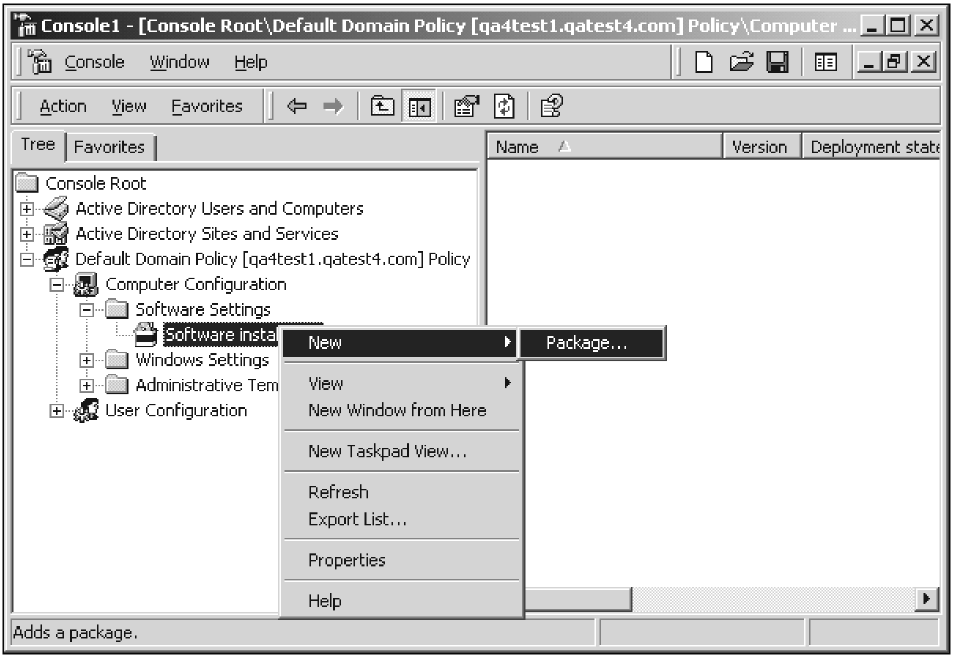
NOTE: You can automatically download Command AntiVirus upgrades, and then create an administrative image using the Command AntiVirus Download Manager. For more information, refer to **Configuring The Download Process** located in the ***COMMANDCentral*** chapter of this guide.

Adding the Command AntiVirus Upgrade Package to Group Policy

Before you can install the Command AntiVirus upgrade, you must add the upgrade package and any MST files that you have created for the upgrade to the group policy that you selected for Command AntiVirus.

To add the Command AntiVirus upgrade package to the selected group policy, follow these steps:

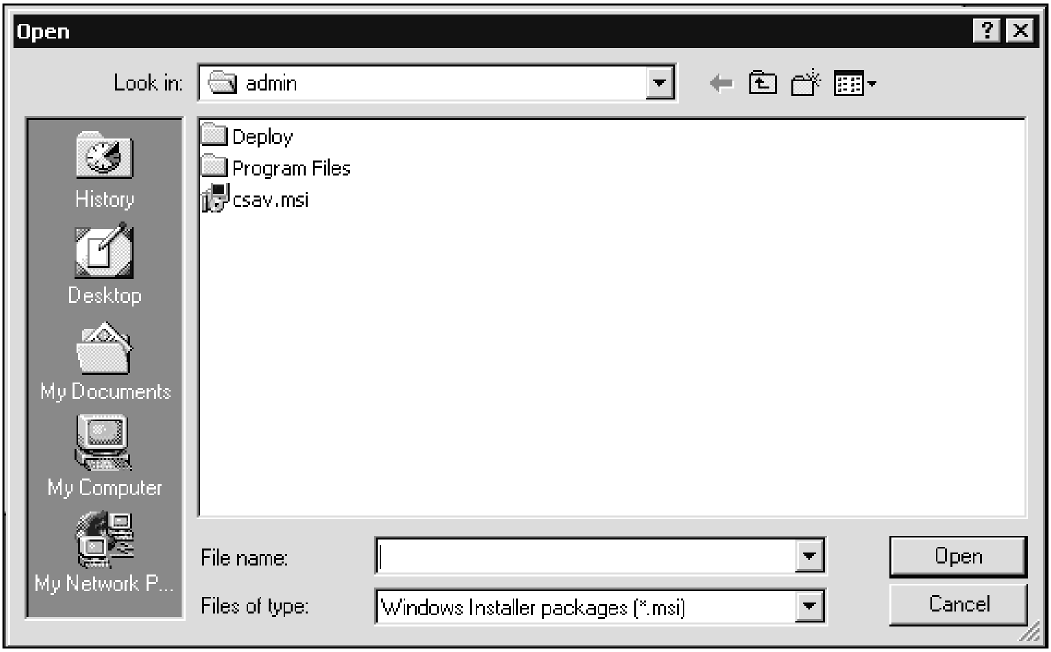
1. In the **Console Root Tree** of the **Microsoft Management Console**, click the plus sign next to the Group Policy object that you selected for Command AntiVirus. This action expands this item. Then, expand **Computer Configuration** and **Software Settings**.
2. Right-click **Software Installation**. The system displays a drop-down menu:



Adds a package.

Software Installation Drop-down Menu

3. Select **New**, and click **Package...**. The system displays the **Open** dialog box:


Look in: admin

Deploy
Program Files
csav.msi

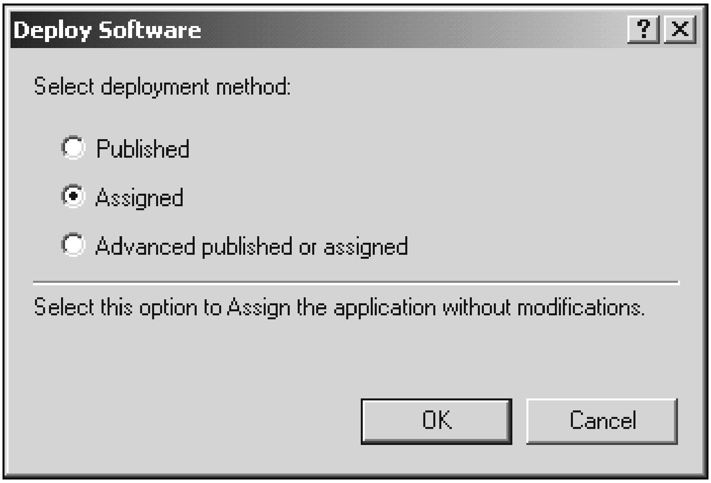
File name:

Files of type: Windows Installer packages (*.msi)

Open Dialog Box

4. Select the **CSAV.MSI** Windows installer upgrade package in the shared network folder, and click **Open**. The system displays the **Deploy Software** dialog box.

NOTE: Make sure that the upgrade package is an administrative image. For more information on installing Command AntiVirus for Windows to a central location on a network, refer to **Installing Command AntiVirus to a Software Distribution point (SDP)** located previously in this chapter.



Select deployment method:

○ Published
● Assigned
○ Advanced published or assigned

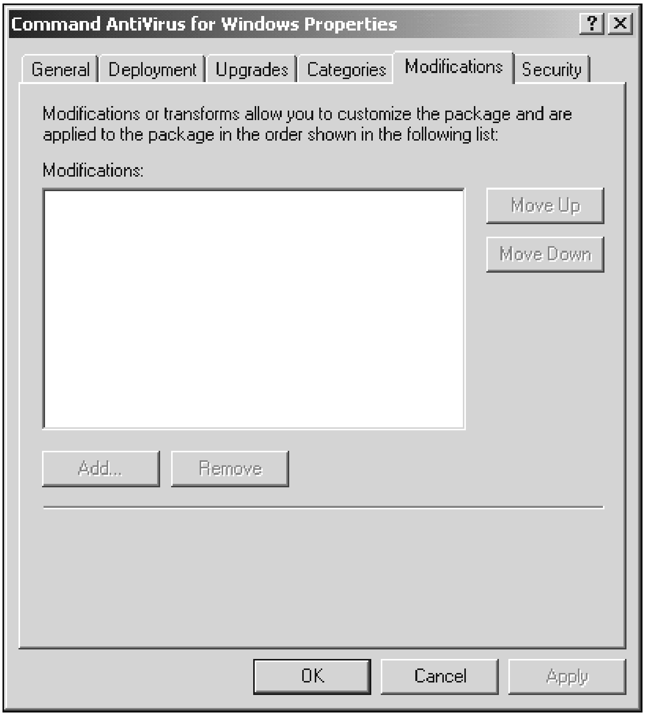
Select this option to Assign the application without modifications.

Deploy Software Dialog Box

5. If you are deploying a **Typical** installation, select **Assigned** and click **OK**. The system returns to the **Microsoft Management Console**. Your deployment is complete. Command AntiVirus will be installed to the computers that you have selected the next time the computer is started.

   If you are deploying a **Custom** installation, select **Advanced published or assigned**, and click **OK**. The system displays the Command AntiVirus for Windows **Properties** dialog box.

6. Click the **Modifications** tab. The system displays the **Modifications** dialog box:



Modifications or transforms allow you to customize the package and are applied to the package in the order shown in the following list:

Modifications Dialog Box

7. Click **Add**. The system displays the **Open** dialog box.
8. Select the **CSAV.MST** file for the upgrade package in the shared network folder, and click **Open**. The system returns to the **Modifications** dialog box.

   Repeat **Steps 7** and **8** for all other MST files that you want to add.

NOTE: Do not click **OK** until you have added all MST files in their proper order. You can use the **Move Up** and **Move Down** buttons to change the order of the files.

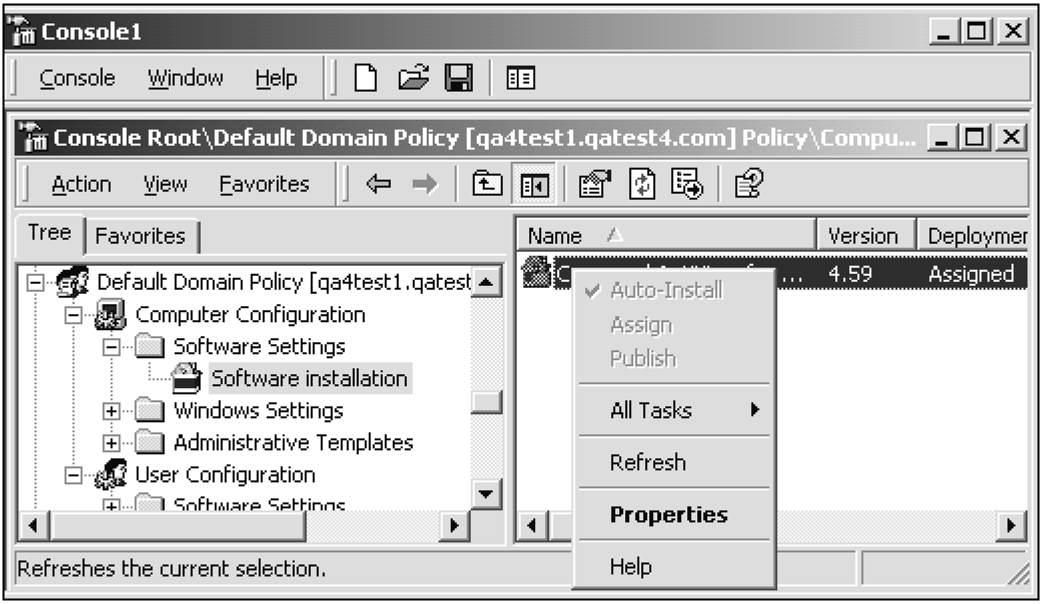
9. Click **OK**. The system returns to the **Microsoft Management Console**.

10. Proceed to **Distributing the Command AntiVirus Upgrade Package**.

Distributing the Command AntiVirus Upgrade Package

To distribute the Command AntiVirus upgrade follow these steps:

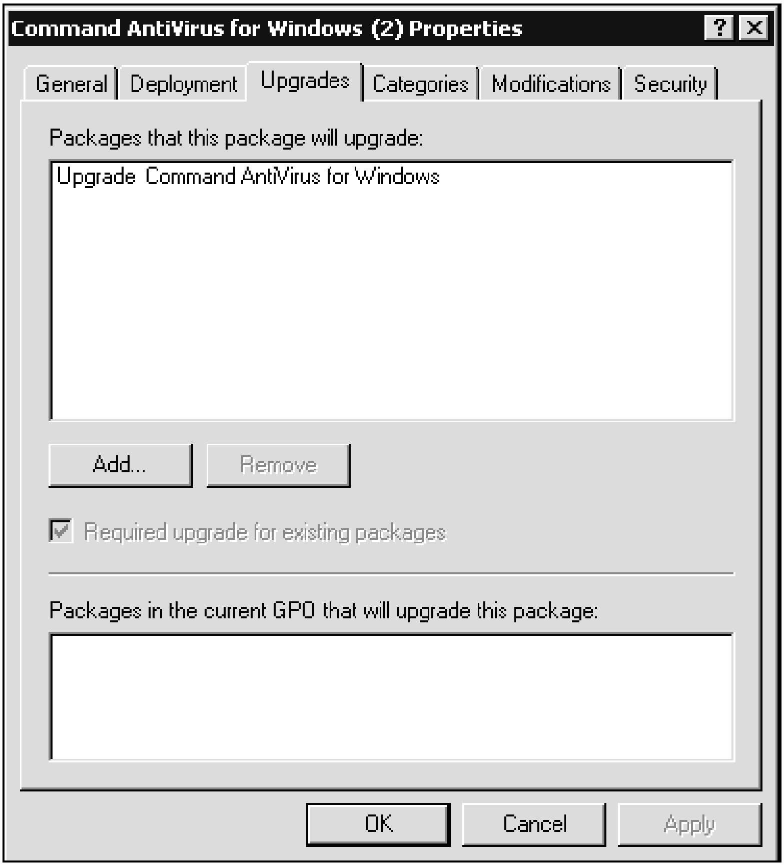
1. In the **Console Root Tree** of the **Microsoft Management Console**, click the plus sign next to the Group Policy object that you selected for Command AntiVirus. This action expands this item. Then, expand **Computer Configuration** and **Software Settings**.
2. Double-click **Software Installation**. The right-hand pane now lists the original Command AntiVirus package and the upgrade package.
3. Right-click the **Command AntiVirus upgrade package**. The system displays a drop-down menu:



Refreshes the current selection.

Package Drop-down Menu

4. Click **Properties**. The system displays the **Command AntiVirus for Windows (2) Properties** dialog box.
5. Click the **Upgrades** tab. The system displays the **Upgrades** dialog box:


Command AntiVirus for Windows (2) Properties

Packages that this package will upgrade:

Upgrade Command AntiVirus for Windows

☑ Required upgrade for existing packages

Packages in the current GPO that will upgrade this package:

Upgrades Dialog Box

6. In the **Packages that this package will upgrade** list, select **Upgrade Command AntiVirus for Windows**.
7. If you want to require users to upgrade to the new package, select the **Required upgrade for existing packages** check box.
8. Click **OK**.

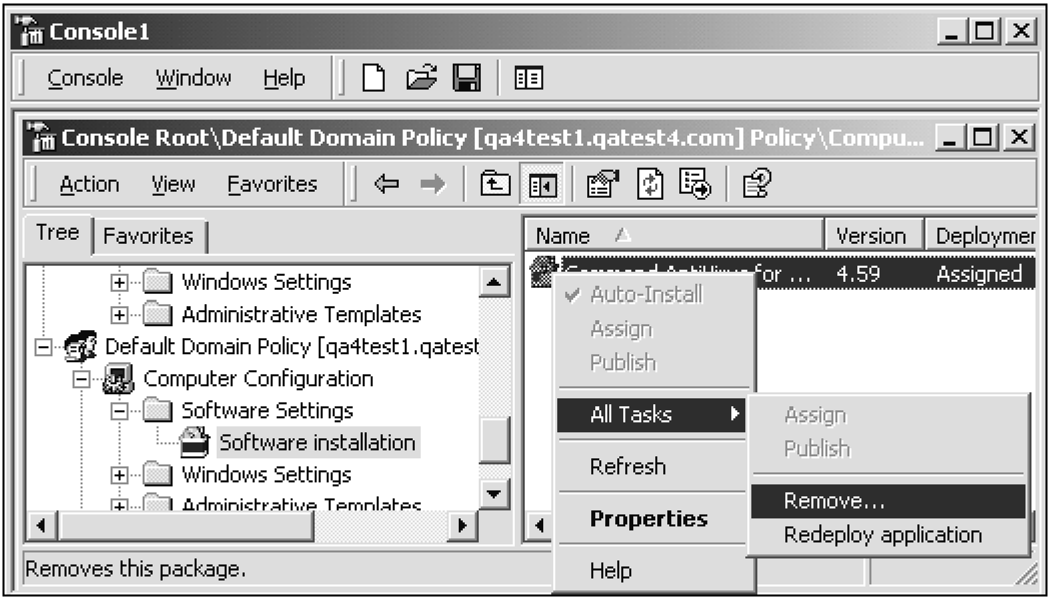
Your deployment is complete. The upgraded version of Command AntiVirus is reinstalled onto the computers that were specified in the original deployment configuration the next time the computer is started.

Removing Command AntiVirus

You can also use Group Policy to remove Command AntiVirus for Windows from individual computers on your network or to stop installing it onto new computers.

To remove or to stop the installation of Command AntiVirus for Windows, follow these steps:

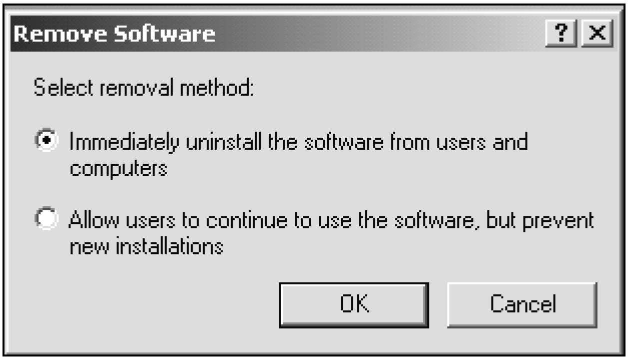
1. In the **Console Root Tree** of the **Microsoft Management Console**, click the plus sign next to the Group Policy object that you selected for Command AntiVirus. This action expands this item. Then, expand **Computer Configuration** and **Software Settings**.
2. Double-click **Software Installation**. The right-hand pane now lists Command AntiVirus.
3. Right-click **Command AntiVirus**. The system displays a drop-down menu:



Removes this package.

Package Drop-down Menu – All Tasks

4. Select **All Tasks** and click **Remove**. The system displays the **Remove Software** dialog box:



Select removal method:

● Immediately uninstall the software from users and computers

○ Allow users to continue to use the software, but prevent new installations

Remove Software Dialog Box

5. Select **one** of the following removal methods, and click **OK**:

   - **Immediately uninstall the software from users and computers** – Removes Command AntiVirus the next time the computer restarts.
   - **Allow users to continue to use the software, but prevent new installations** – Allows users who are currently using Command AntiVirus to continue using it and to perform repairs, but does not allow any new installations.

UPDATING COMMAND ANTIVIRUS

To provide protection against new viruses, we update the Command AntiVirus definition files (deffiles) frequently. You can schedule automatic downloads of the deffiles, component updates, and full product upgrades using the Command AntiVirus Download Manager that is part of COMMANDCentral.

The Command AntiVirus Download Manager also allows you to apply the deffile and component updates to administrative images automatically. Command AntiVirus for Windows contains an agent that detects a change in the administrative image. When you apply the updates to the administrative image, CSAV with the updated files is reinstalled onto the computers that were specified in the original deployment configuration the next time the user logs on to the machine.

Full product upgrades are similar to new installations, you must create a new administrative image and then customize, advertise, and deploy CSAV.

The Download Manager allows you to create an administrative image of a downloaded upgrade of Command AntiVirus. You can create this administrative image on a single server or on multiple servers by creating a directory share. From these multiple Software Distribution Points (SPDs), you can then advertise Command AntiVirus.

For information on creating multiple SDPs from which you can advertise Command AntiVirus, refer to **Creating an Administrative Image of a Downloaded Upgrade** located in the ***COMMANDCentral*** chapter of this guide.

For more information on configuring and scheduling downloads, refer to **Configuring The Download Process** located in the ***COMMANDCentral*** chapter of this guide.

2K/XP

If you are updating Windows 2000 and Windows XP machines that have Active Directory installed, you can also apply the updated deffiles manually using Active Directory. For more information, refer to **Starting the Installation Process** located previously in this chapter.

RUNNING A DOS SCAN AT LOGIN

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

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

```
DOS SET FP-DATA=”C:\F-PROT.DAT”

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

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

COMMANDCENTRAL

COMMANDCentral is a centralized management package that allows administrators to prepare the Command AntiVirus (CSAV) installation for deployment across the network from one location.

NOTE: COMMANDCentral can be used to administer **only** Command AntiVirus for Windows® Version 4.70 and later.

COMMANDCentral contains the following administrative tools that allow you to download Command AntiVirus updates and upgrades, deploy the Command AntiVirus Pre-installation Convenience Pack to machines across your network, customize features and settings prior to deploying CSAV, and advertise CSAV across your network. All of the tools are installed by default.

- **Command AntiVirus Deployment Prep Wizard** – Allows you to deploy the CSS Remote Agent, install the Command AntiVirus Pre-installation Convenience Pack, create an administrative image, create a customized transform file (.MST), and advertise CSAV across your network.

If you are using **only** Active Directory to customize and deploy Command AntiVirus across your network, you do not need to use this wizard.

NOTE: A shortcut to the CSAV Deployment Prep Wizard is created in the COMMANDCentral folder of the Windows Start menu.

If you are administering your network from a Windows 95/98/Me machine, the Command AntiVirus Deployment Prep Wizard is **not** available.

- **System Policy Template for Windows Installer** – Allows administrators using Windows NT® and Windows 95, Windows 98, and Windows Me to configure the settings for the Windows Installer.
- **System Policy Template for Command AntiVirus** – Allows you to configure the settings for Command AntiVirus.
- **Custom Installation Wizard for Command AntiVirus** – Allows you to customize the Command AntiVirus installation by adding or removing features, creating customized scan tasks, and configuring Command AntiVirus settings. You can also import settings from a previous version of Command AntiVirus.

NOTE: A shortcut to the Custom Installation Wizard is created in the COMMANDCentral folder of the Windows Start menu.

- **Command AntiVirus Download Manager** – allows you to download Command AntiVirus updates and upgrades and to apply them to administrative images.

NOTE: A shortcut to the CSAV Download Manager is created in the COMMANDCentral folder of the Windows Start menu.

The deployment method you chose to install Command AntiVirus across your network and your need to schedule downloads, determines what tools you should use. For more information on your deployment options, refer to the ***Network Administration*** chapter of this administrator’s guide.

SYSTEM REQUIREMENTS

To install and operate COMMANDCentral, you must have:

- At least **one** of the following Microsoft Windows 32-bit platforms installed:

  Windows NT® 4.0 with Service Pack 4 or higher

  Windows NT® Server edition 4.0 with Service Pack 4 or higher

  Windows 2000 Professional

  Windows 2000 Server

  Windows 2000 Advanced Server

  Windows XP Professional

  Windows XP Home

- Microsoft Internet Explorer 5.0 or higher installed
- Windows Active Directory Service Interface (ADSI) client

NOTE: The ADSI client program is packaged with the COMMANDCentral installation files. To install the client, double-click the **ADS.EXE** file.

COMMANDCentral installs on a Windows 95/98/Me machine, but the Command AntiVirus Deployment Prep Wizard is **not** available.

INSTALLATION

The following instructions will help you to install COMMANDCentral quickly and easily. The default installation installs all of the required components.

We suggest that you read through these instructions prior to installing the product. This will allow you to better anticipate any choices that you may need to make during the installation process.

INSTALLING

To install and use COMMANDCentral on Windows NT, Windows 2000, or Windows XP, **one** of the following conditions **must** be met:

- You are a member of the Administrators group on the local machine
- System policy is set so that you have elevated privileges for installations

NOTE: The COMMANDCentral installation is in a 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 **CCOMMAND.MSI**.

After installing the Windows Installer, the user may need to restart the computer. After the computer restarts, Setup continues.

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

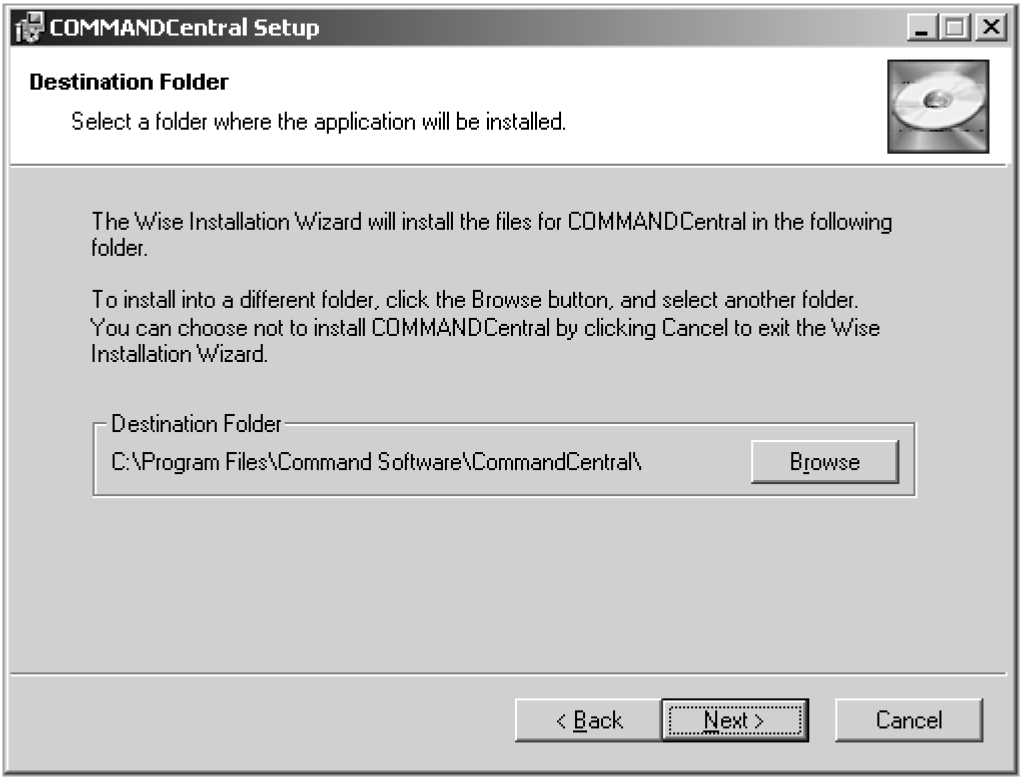
To install COMMANDCentral, follow these steps:

1. Insert the CD-ROM.
2. Click the **Start** button on the Windows task bar.
3. Click **Run**.

4. Click **Browse** to search the CD for the **COMMANDC** folder.
5. Open that folder.
6. In the **File of type** drop-down, select **All Files**.
7. To run the setup program, double-click **SETUP.EXE**.

   The system returns to the **Run** dialog box.

8. Click **OK**. The system displays the **Welcome** dialog box.
9. Click **Next**. The system displays the **License Agreement**.
10. To accept the license agreement, select **I accept the License Agreement**, and click **Next**. The system displays the **Destination Folder** dialog box:



Destination Folder

Select a folder where the application will be installed.

The Wise Installation Wizard will install the files for COMMANDCentral in the following folder.

To install into a different folder, click the Browse button, and select another folder. You can choose not to install COMMANDCentral by clicking Cancel to exit the Wise Installation Wizard.

Destination Folder

C:\Program Files\Command Software\CommandCentral\

Destination Folder Dialog Box

11. In the **Destination Folder** text box, type where you want the files installed. The default is: `C:\Program Files\Command Software\CommandCentral`

NOTE: You can use the **Browse** button to select a different folder.

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

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

When the copying is complete, the system displays a dialog box informing you that COMMANDCentral has been successfully installed.

13. Click **Finish** to exit.

PREPARING FOR DEPLOYMENT

Before you can install Command AntiVirus across your network, there are several steps that you need to take to prepare for the installation. For more information, refer to **Preparing For The Installation** located in the ***Network Administration*** chapter of this administrator's guide.

The Command AntiVirus Deployment Prep Wizard allows administrators with mixed environments to prepare the network for the deployment of Command AntiVirus 4.70 or higher quickly and easily. Using this wizard you can perform the following tasks.

NOTE: If you are administering your network from a Windows 95/98/Me machine, the Command AntiVirus Deployment Prep Wizard is **not** available. For more information, refer to **Recommended Methods For 9x Only Networks** located in the ***Network Administration*** chapter of this administrator's guide.

- Install the Command AntiVirus Pre-installation Convenience Pack onto Windows NT machines across your network

95/98/Me

You can install the Command AntiVirus Pre-installation Convenience Pack onto Windows 95/98/Me machines by placing the **CSS Remote Agent RunP** that is created by the wizard in an e-mail or logon script. For more information, refer to **Starting The Installation Process** located in the ***Network Administration*** chapter of this administrator's guide.

- Perform an administrative installation to a Software Distribution Point (SDP)
- Customize CSAV features and settings
- Advertise CSAV across your network

COMMAND ANTIVIRUS DEPLOYMENT PREP WIZARD

✓ **NOTE:** If you are administering your network from a Windows 95/98/Me machine, the Command AntiVirus Deployment Prep Wizard is **not** available. For more information, refer to **Recommended Methods For 9x Only Networks** located in the ***Network Administration*** chapter of this administrator's guide.

2K/XP

If you are using **only** Active Directory to customize and deploy Command AntiVirus across your network, you do **not** need to use this wizard.

95/98/Me

If you are administering Windows 95/98/Me machines, click the link in the **Welcome** dialog box of the wizard to find out more about Windows 95/98/Me workstation administration.

Using this wizard you can:

- Deploy the CSS Remote Agent from a network server on to selected machines.

  This agent allows you to install the prerequisite component files (Command AntiVirus Pre-installation Convenience Pack) and to apply administrative rights to install (advertise) to the CSAV installation package.

- Install the prerequisite component files that prepare the machines for the installation of CSAV.

You can install the Command AntiVirus Pre-installation Convenience Pack onto Windows 95/98/Me machines by placing the CSS Remote Agent RunP that is created by the wizard in an e-mail or logon script. For more information, refer to **Starting the Installation Process** located in the ***Network Administration*** chapter of this administrator's guide.

- Create an administrative image. These are the files created from performing an administrative installation to a shared network folder (SDP).
- Create a customized transform file (.MST).
- Advertise CSAV across your network.

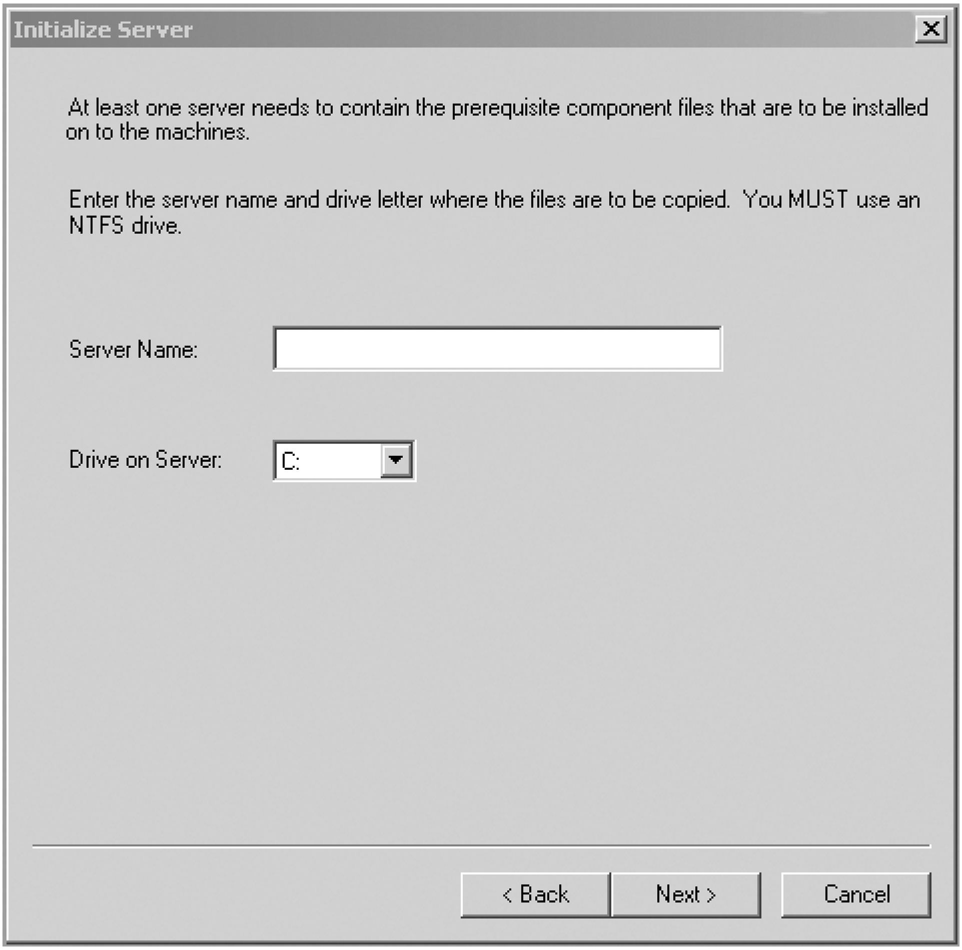
The wizard is easy to use. Just make your selections, and click **Next** to continue. If you do not need to perform the specified action on a page, you can select the **Skip Page** check box to go to the next page.

Here are just a few points to remember.

- To go back to the previous dialog box, click **Back**.
- To exit the wizard during the process, click **Cancel**.
- To exit the wizard after you have completed the process, click **Finish**.

To start the wizard, follow these steps:

1. Click the **Start** button on the Windows taskbar.
2. Select **Programs**.
3. Select **COMMANDCentral**.
4. Click **Command AntiVirus Deployment Prep Wizard**. The system displays the **Welcome** dialog box.
5. Click **Next**. The system displays the **Initialize Server** dialog box:


Initialize Server

At least one server needs to contain the prerequisite component files that are to be installed on to the machines.

Enter the server name and drive letter where the files are to be copied. You MUST use an NTFS drive.

Server Name:

Drive on Server: C:

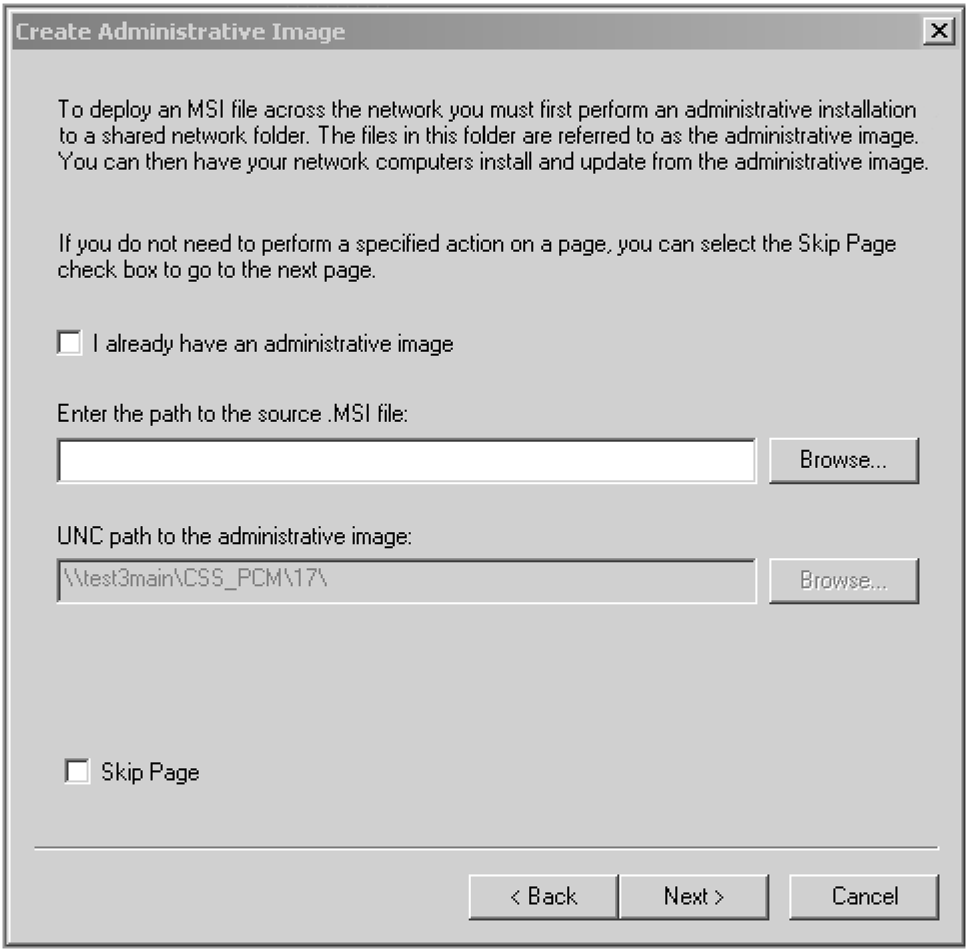
Initialize Server Dialog Box

NOTE: At least **one** server needs to contain the prerequisite component files that are to be installed onto the machines.

6. In the **Server Name** text box, type the name of the server where the prerequisite component files are to be copied.
7. In the **Drive on Server** text box, click the drop-down arrow to select the drive letter.

NOTE: You **<u>must</u>** select an NTFS drive.

8. Click **Next**. The system displays the **Create Administrative Image** dialog box:



Create Administrative Image

To deploy an MSI file across the network you must first perform an administrative installation to a shared network folder. The files in this folder are referred to as the administrative image. You can then have your network computers install and update from the administrative image.

If you do not need to perform a specified action on a page, you can select the Skip Page check box to go to the next page.

□ I already have an administrative image

Enter the path to the source .MSI file:

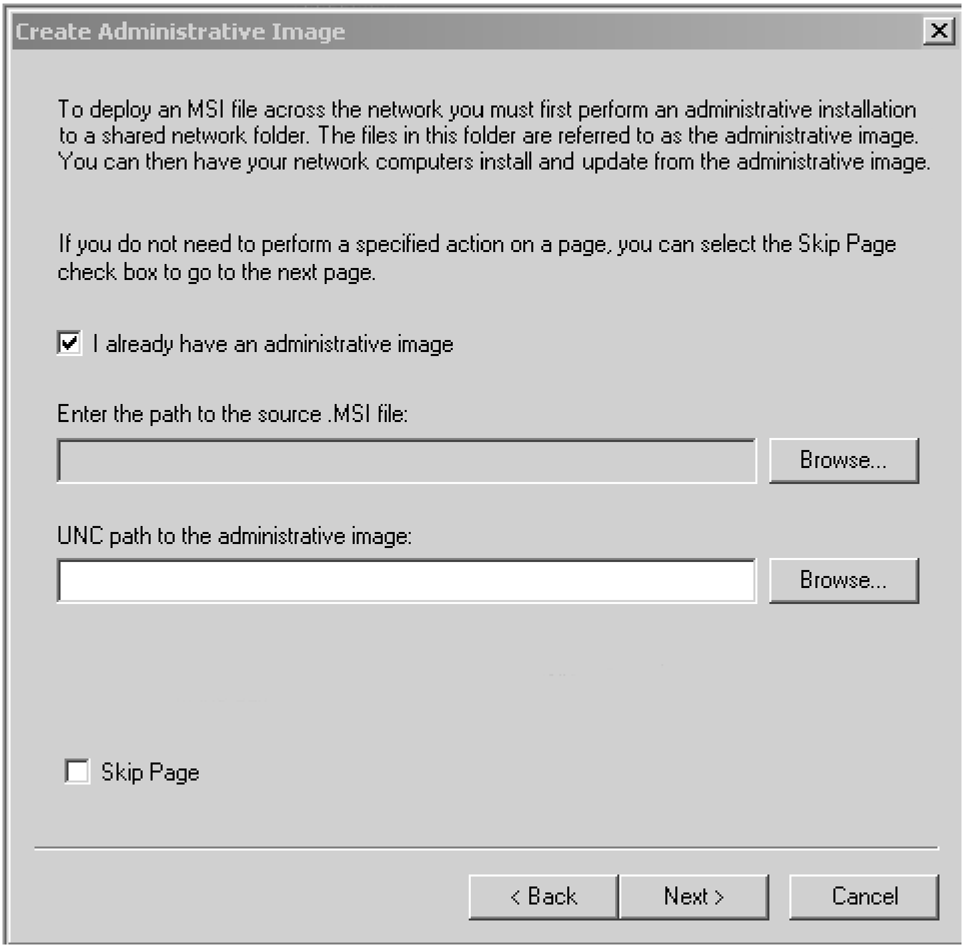
UNC path to the administrative image: \\test3main\CSS_PCM\17\

□ Skip Page

Create Administrative Image Dialog Box

This dialog box allows you to perform an administrative installation to a shared network folder. The folder is referred to as the Software Distribution Point (SDP). The files in the folder are referred to as the administrative image. You can then have your network computers install and update from the administrative image.

9. Select **<u>one</u>** of the following options:
   - If you have an administrative image – Select the **I already have an administrative image** check box.



Create Administrative Image

To deploy an MSI file across the network you must first perform an administrative installation to a shared network folder. The files in this folder are referred to as the administrative image. You can then have your network computers install and update from the administrative image.

If you do not need to perform a specified action on a page, you can select the Skip Page check box to go to the next page.

☑ I already have an administrative image

Enter the path to the source .MSI file:

UNC path to the administrative image:

☐ Skip Page

Create Administrative Image Dialog Box

- If you do **not** have an administrative image – In the **Enter the path to the source .MSI file** text box, type the path to the Command AntiVirus .MSI file.

NOTE: You can use the **Browse** button to search for the file.

10. In the **UNC path to the administrative image text box**, type the path to the SDP.

NOTE: You can use the **Browse** button to search for the folder. We recommend using a Universal naming Convention (UNC) path.

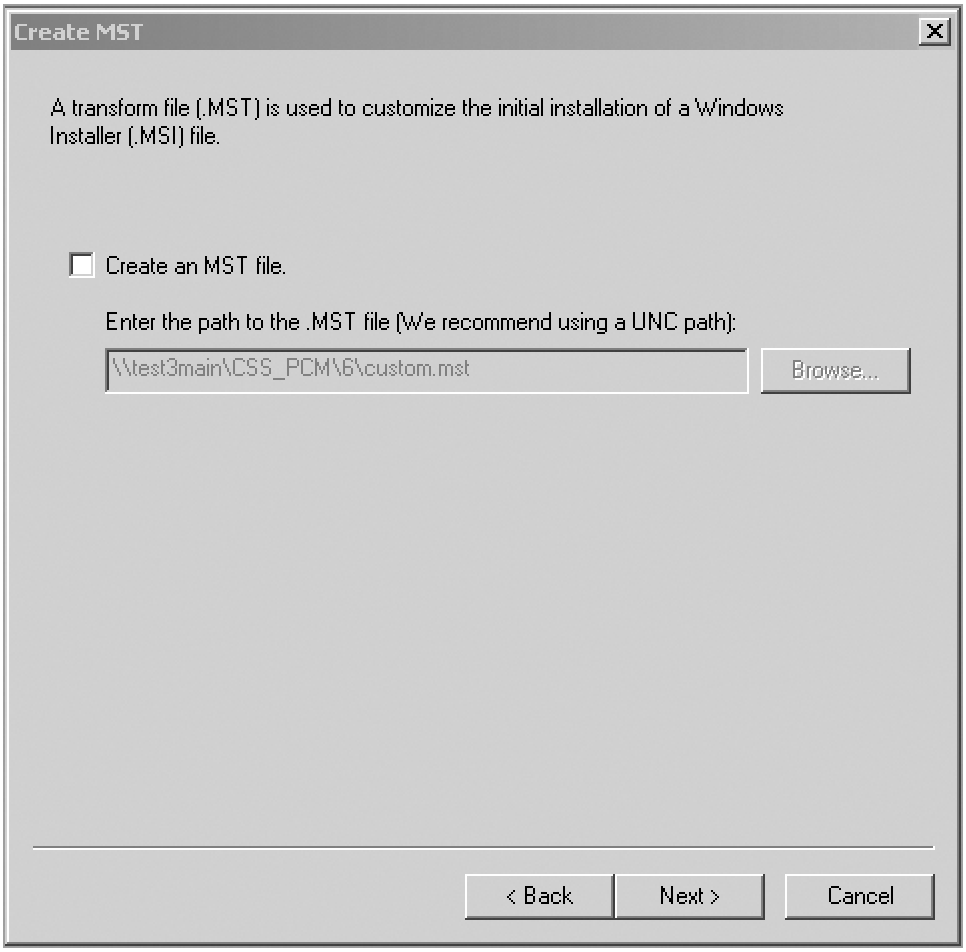
If you did not already have an administrative image, the wizard automatically generates a folder to store the administrative image. This folder is created on the server and the NTFS drive that you previously selected. The path to the folder is displayed under **UNC path to the administrative image**. You can accept this default path or browse to another folder.

11. Click **Next** to begin creating the administrative image. The system displays the **Updating System** dialog box. Please wait while the program copies the files to the SDP.

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

We recommend that you copy the administrative image to another location in your network. This provides a backup copy when an installation needs to be repaired. This copy is **only** for backup purposes. Command AntiVirus can only be installed from the location from which it was advertised.

When the copying is complete, the system displays the **Create MST** dialog box:



Create MST

A transform file (.MST) is used to customize the initial installation of a Windows Installer (.MSI) file.

□ Create an MST file.

Enter the path to the .MST file (We recommend using a UNC path):

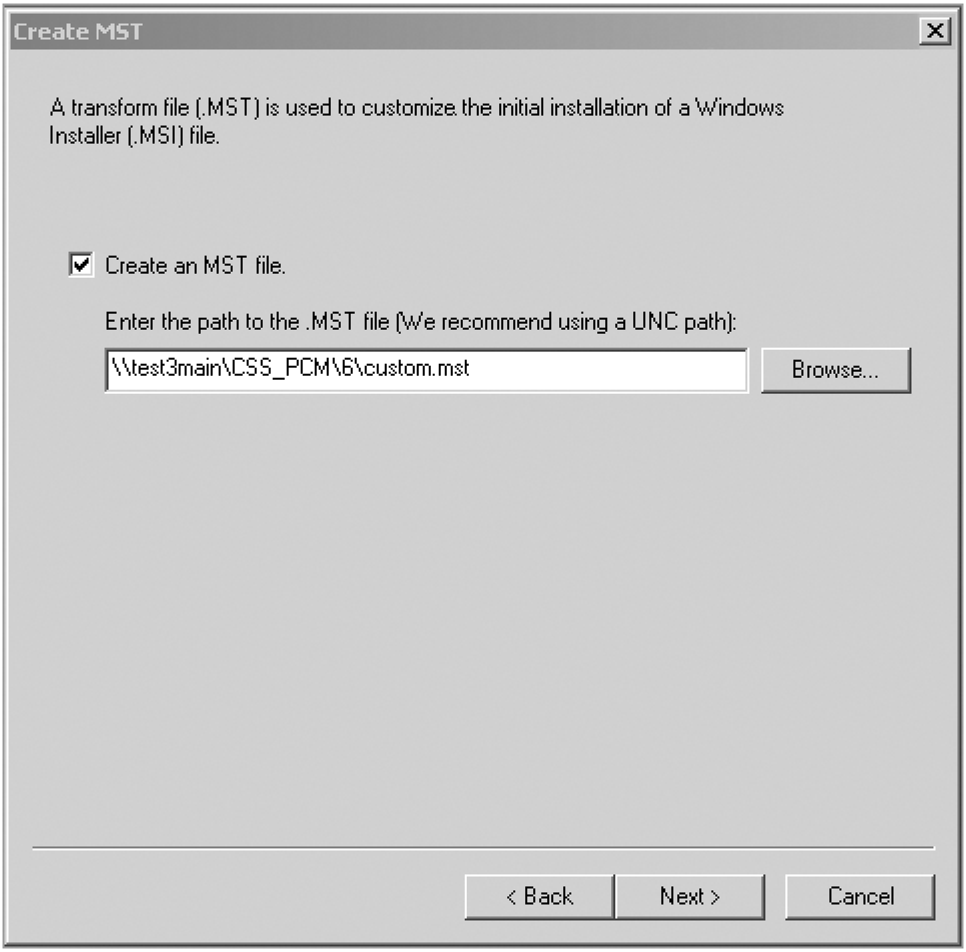
\\test3main\CSS_PCM\6\custom.mst

Create MST Dialog Box

This dialog box allows you to create a custom Windows installer transform (MST file). The MST file contains your customized installation features and settings.

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

    - If you do **not** want to customize CSAV, click **Next**, and go to **Step 14**.
    - If you want to create an MST file, select the **Create an MST file** check box. The system redisplays the **Create MST** dialog box with the **Enter the path to the .MST file** text box active:



Create MST

A transform file (.MST) is used to customize the initial installation of a Windows Installer (.MSI) file.

☑ Create an MST file.

Enter the path to the .MST file (We recommend using a UNC path):

\\test3main\CSS_PCM\6\custom.mst

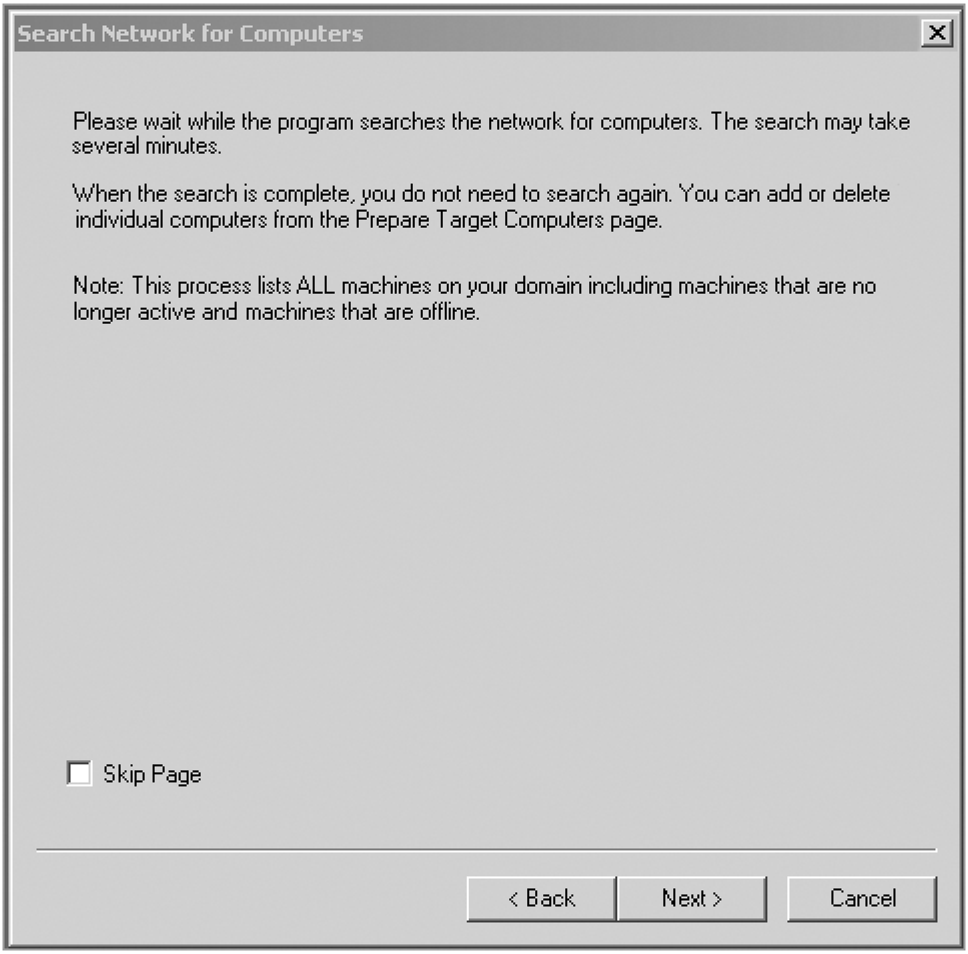
Create MST Dialog Box - Path Available

You can accept the default path or use the **Browse** button to select a new path. We recommend using a Universal Naming Convention (UNC) path.

13. Click **Next**. The system displays the Custom Installation Wizard for Command AntiVirus **Welcome** dialog box.

    Follow the instructions on the screens to complete the customization. For more information, refer to **Custom Installation Wizard** located later in this chapter.

14. The system displays the **Search Network for Computers** dialog box:



Search Network for Computers

Please wait while the program searches the network for computers. The search may take several minutes.

When the search is complete, you do not need to search again. You can add or delete individual computers from the Prepare Target Computers page.

Note: This process lists ALL machines on your domain including machines that are no longer active and machines that are offline.

☐ Skip Page

Search Network for Computers Dialog Box

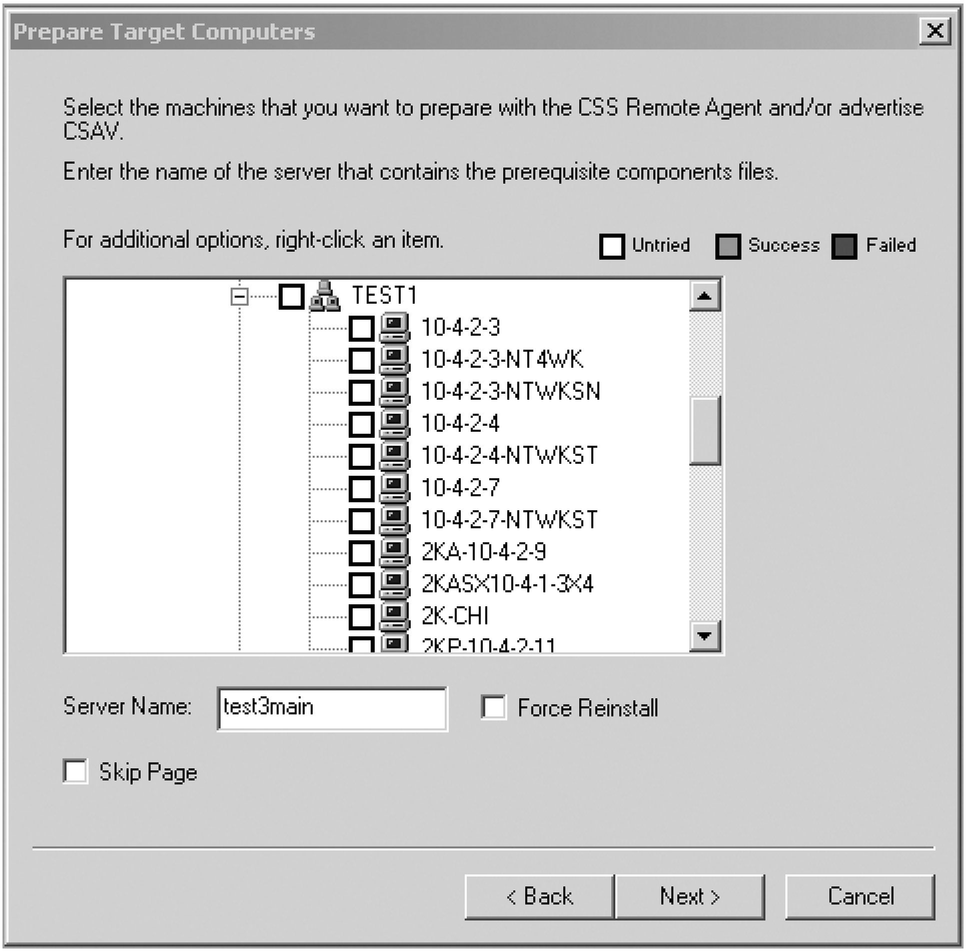
15. Click **Next** to continue.

    Please wait while the program searches the network for computers. The search may take several minutes.

NOTE: This process lists **all** of the machines on your domain including machines that are no longer active and machines that are offline.

When the search is complete, the system displays the **Prepare Target Computers** dialog box.

NOTE: You do **not** need to search again. You can add or delete individual computers from the **Prepare Target Computers** dialog box:



Prepare Target Computers

Select the machines that you want to prepare with the CSS Remote Agent and/or advertise CSAV.

Enter the name of the server that contains the prerequisite components files.

For additional options, right-click an item.

Server Name: test3main

☐ Force Reinstall

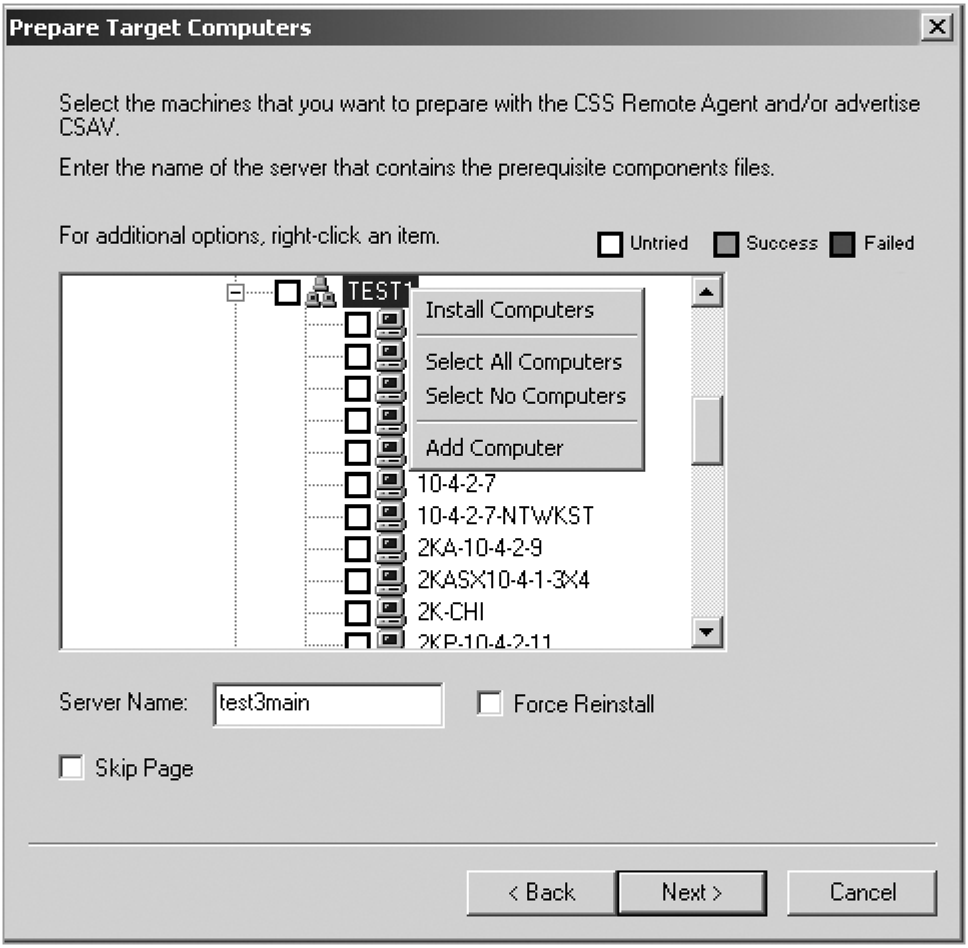
☐ Skip Page

Prepare Target Computers Dialog Box

16. In the **Target Computers** list, select the machines on which you want to install the CSS Remote Agent. You can also select the machines on which you want to advertise CSAV. Click the plus sign (**+**) to the left of a domain to expand it, for example, **TEST1**.

    You can select an entire domain or individual machines by clicking the check box to the left of the domain or machine name. For example, to select **all** of the machines in the **TEST1** domain, click the check box to the left of **TEST1**.

    You can also click **Select All Computers** from the drop-down menu. Using the right mouse button (right-click), click a domain name. The system displays a drop-down menu:



Prepare Target Computers

Select the machines that you want to prepare with the CSS Remote Agent and/or advertise CSAV.

Enter the name of the server that contains the prerequisite components files.

For additional options, right-click an item.

□ Untried ▨ Success ■ Failed

Server Name: test3main

□ Force Reinstall

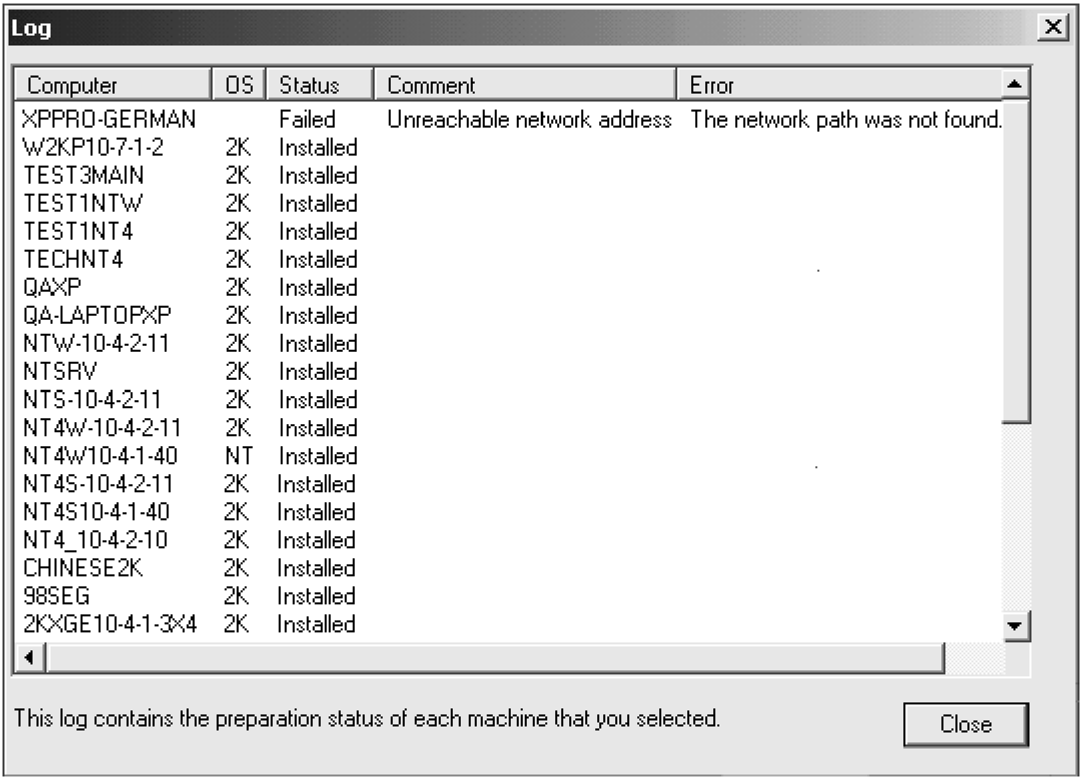
□ Skip Page

Prepare Target Computers – Domain Drop-down Menu

From this menu you can:

- **Install Computers** – Installs the prerequisite components on the machines that you selected in that particular domain.
- **Select All Computers** – Selects **all** machines in that particular domain
- **Select No Computers** – Clears **all** selected machines in that particular domain.
- **Add Computer** – Adds a computer to the **Target Computers** list for that particular domain.

17. In the **Server Name** text box, type the name of the server that contains the prerequisite component files.
18. Click **Next**. Please wait while the machines are prepared. When the preparation is complete, the system displays the **Log**:



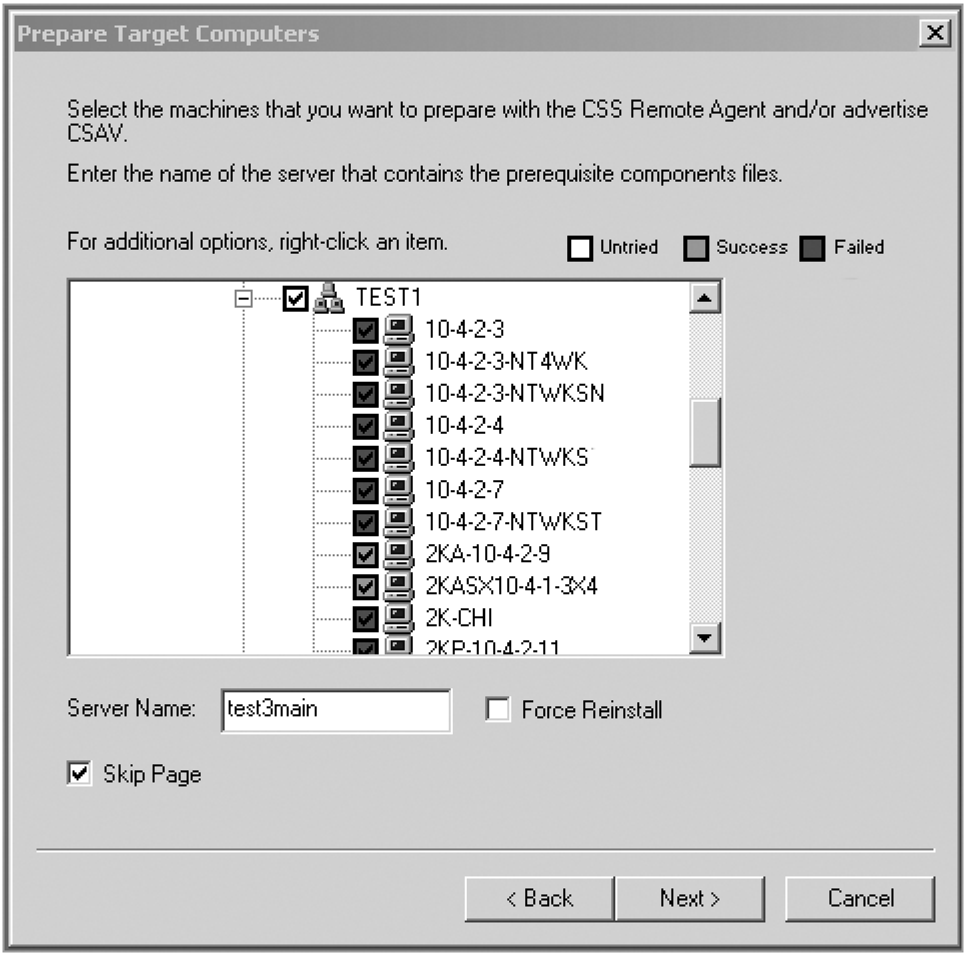
Computer	OS	Status	Comment	Error
XPPRO-GERMAN		Failed	Unreachable network address	The network path was not found.
W2KP10-7-1-2	2K	Installed		
TEST3MAIN	2K	Installed		
TEST1NTW	2K	Installed		
TEST1NT4	2K	Installed		
TECHNT4	2K	Installed		
QAXP	2K	Installed		
QA-LAPTOPXP	2K	Installed		
NTW-10-4-2-11	2K	Installed		
NTSRV	2K	Installed		
NTS-10-4-2-11	2K	Installed		
NT4W-10-4-2-11	2K	Installed		
NT4W10-4-1-40	NT	Installed		
NT4S-10-4-2-11	2K	Installed		
NT4S10-4-1-40	2K	Installed		
NT4_10-4-2-10	2K	Installed		
CHINESE2K	2K	Installed		
98SEG	2K	Installed		
2KXGE10-4-1-3X4	2K	Installed		

This log contains the preparation status of each machine that you selected.

Log

This log contains details of the installation on each machine that you selected. It specifies the computer name, the operating system, whether it installed or failed. If applicable, it also specifies the reason for a failure and the error that occurred.

19. Click **Close**. The system returns to the **Prepare Target Computers** dialog box:



Prepare Target Computers

Select the machines that you want to prepare with the CSS Remote Agent and/or advertise CSAV.

Enter the name of the server that contains the prerequisite components files.

For additional options, right-click an item.

□ Untried ▨ Success ■ Failed

- ☑ TEST1
  - ☑ 10-4-2-3
  - ☑ 10-4-2-3-NT4WK
  - ☑ 10-4-2-3-NTWKSN
  - ☑ 10-4-2-4
  - ☑ 10-4-2-4-NTWKS
  - ☑ 10-4-2-7
  - ☑ 10-4-2-7-NTWKST
  - ☑ 2KA-10-4-2-9
  - ☑ 2KASX10-4-1-3X4
  - ☑ 2K-CHI
  - ☑ 2KP-10-4-2-11

Server Name: test3main

□ Force Reinstall

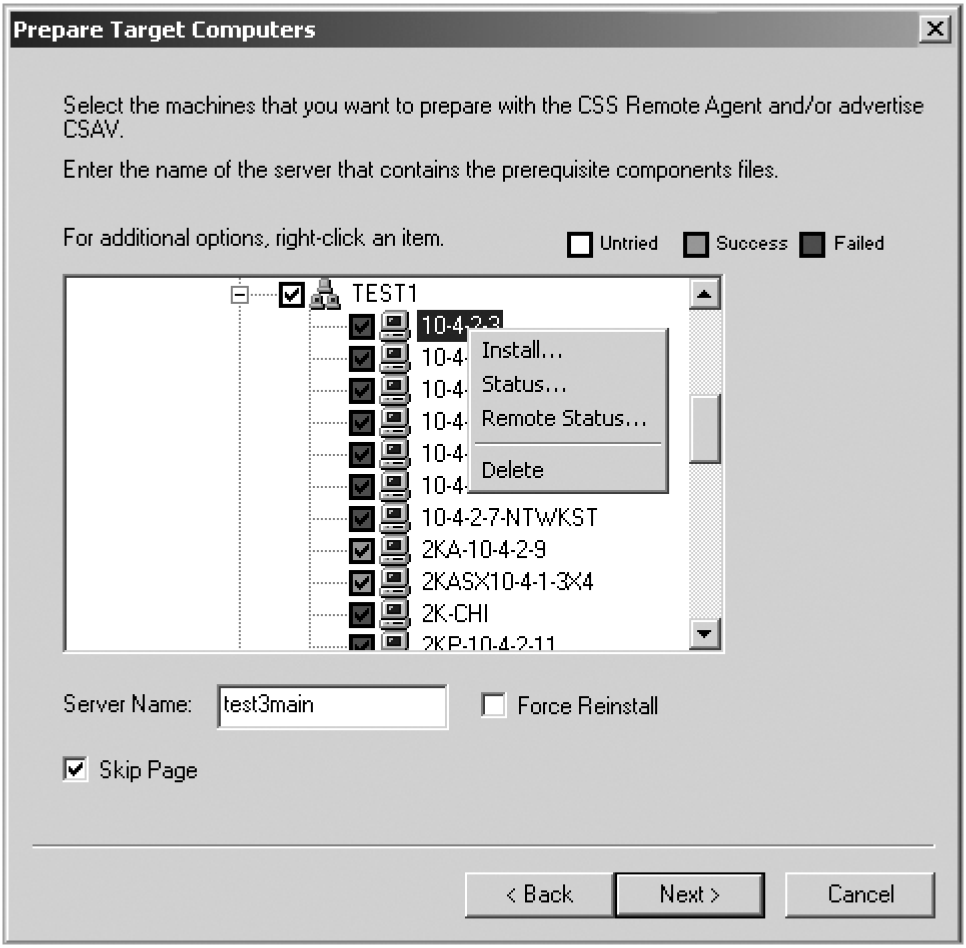
☑ Skip Page

Prepare Target Computers Dialog Box – Machines Selected

The check boxes of the machines that you selected are now color coded to reflect the status of the installation. Green represents a successful installation. Red represents a failed installation.

To reinstall on the selected machines, click the **Force Reinstall** check box.

For additional options, right-click a machine name. The system displays a drop-down menu:



Prepare Target Computers

Select the machines that you want to prepare with the CSS Remote Agent and/or advertise CSAV.

Enter the name of the server that contains the prerequisite components files.

For additional options, right-click an item.

□ Untried ▨ Success ■ Failed

☑ TEST1
- ☑ 10-4-2-3
- ☑ 10-4
- ☑ 10-4
- ☑ 10-4
- ☑ 10-4
- ☑ 10-4
- ☑ 10-4-2-7-NTWKST
- ☑ 2KA-10-4-2-9
- ☑ 2KASX10-4-1-3X4
- ☑ 2K-CHI
- ☑ 2KP-10-4-2-11

Server Name: test3main

□ Force Reinstall

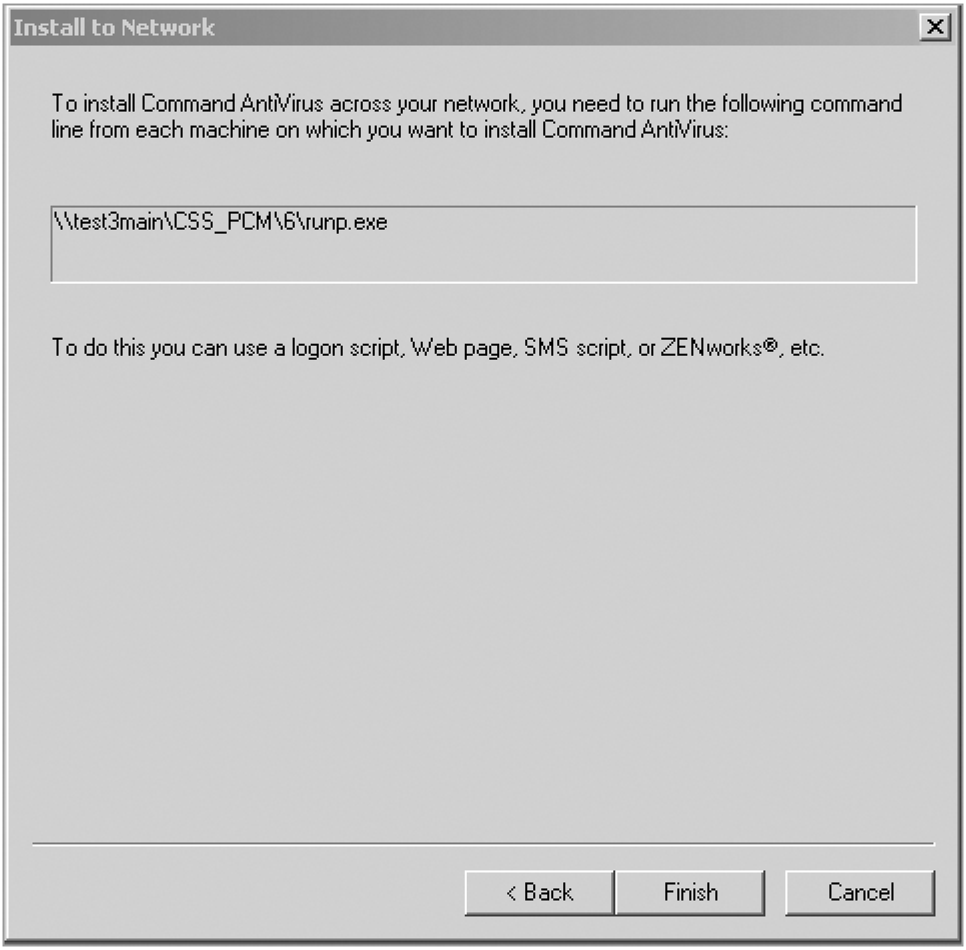
☑ Skip Page

Prepare Target Computers – Machine Drop-down Menu

From this menu, you can select **one** of the following options:

- **Install** – Installs the prerequisite components on that particular machine.
- **Status** – Displays the details of the installation on that particular machine.
- **Remote Status** – Allows you to view the two prerequisite component status files. This allows you to make sure that the prerequisite component files were installed and started correctly.
- **Delete** – Deletes that particular machine from the **Target Computers** list.

20. Click **Next**. The system displays the **Install to Network** dialog box:



Install to Network

To install Command AntiVirus across your network, you need to run the following command line from each machine on which you want to install Command AntiVirus:

\\test3main\CSS_PCM\6\runp.exe

To do this you can use a logon script, Web page, SMS script, or ZENworks®, etc.

Install to Network Dialog Box

This dialog box provides you with a command line that you can copy and paste into a logon script, web page, SMS script, or ZENworks®, etc.

To install Command AntiVirus across your network, you need to run the command line from each machine on which you want to install Command AntiVirus.

⚠ For Windows 95/98/Me machines, you must also include the RunP to install the prerequisite component files.

For more information, refer to **Starting The Installation Process** located in the ***Network Administration*** chapter of this administrator's guide.

21. Click **Finish** to exit the wizard.

CUSTOMIZING YOUR CSAV INSTALLATION SETTINGS

COMMANDCentral contains several tools that allow administrators to customize features and settings prior to deploying Command AntiVirus throughout the network. These tools include the:

- System Policy Template for Windows Installer
- System Policy Template for Command AntiVirus
- Custom Installation Wizard for Command AntiVirus

Using the System Policy templates, you can customize the Windows Installer and the Command AntiVirus settings. You can then apply these settings to computers throughout the network by adding the System Policy Templates to System Policy in Windows NT and Windows 95/98/Me or Group Policy in Windows 2000/XP.

Using the Custom Installation Wizard for Command AntiVirus you can import Command AntiVirus settings from a previous version, add or remove features, and create custom scan tasks. If you are not using the System Policy Template for Command AntiVirus, you can also use the wizard to customize Command AntiVirus settings. The wizard then saves the changes to a Windows Installer transform (**.MST** file) that can be deployed with the Command AntiVirus installation **.MSI** to computers throughout the network.

The following sections describe each tool in detail.

SYSTEM POLICY TEMPLATE FOR WINDOWS INSTALLER

9x/Me/NT

The System Policy Template for Windows Installer (**INSTLR11.ADM**) allows administrators using Windows NT 4.0 and Windows 95/98/Me to set the Windows Installer installation policies for computers on the network. These policies control aspect of the Windows Installer's behavior such as security, logging, and rollback.

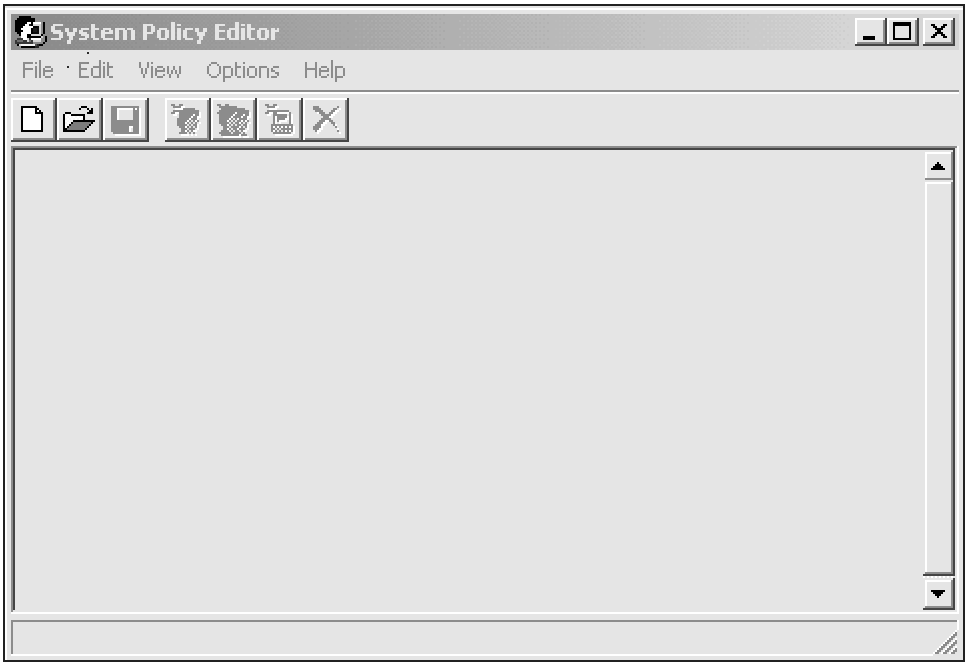
95/98/Me

To use this template on Windows 95/98/Me, you must have SYSPOL and POLEDIT installed.

Once you have added the template to System Policy, you can open the template to configure the installation settings.

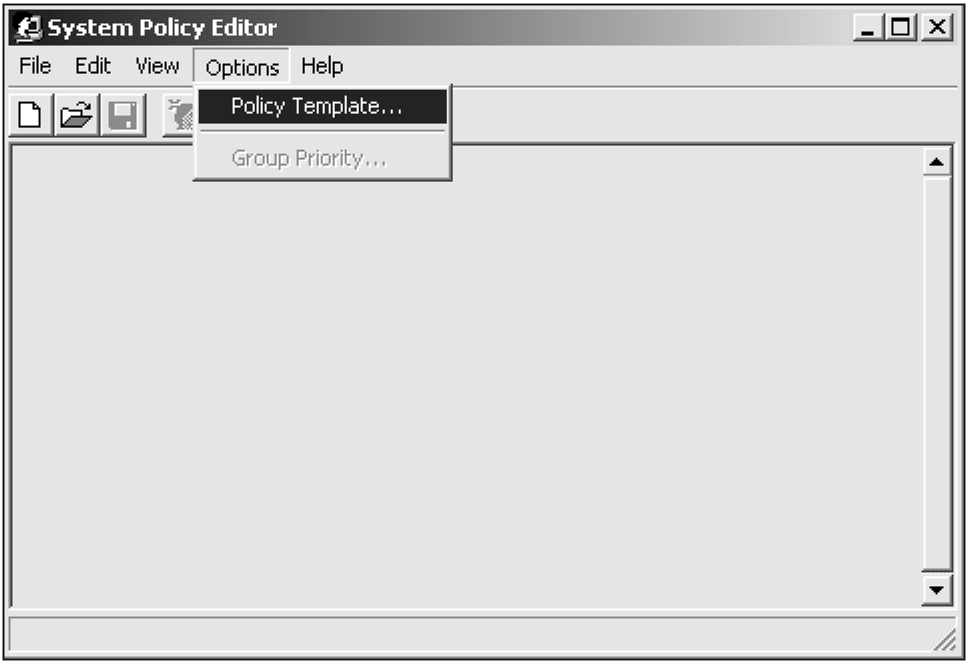
To add the template to **Policy Template Options** in System Policy and customize the Windows Installer settings, follow these steps:

1. Click the **Start** button on the Windows task bar.
2. Click **Run**.
3. In the text box, type **poledit**.
4. Click **OK**. The system displays the System Policy Editor:



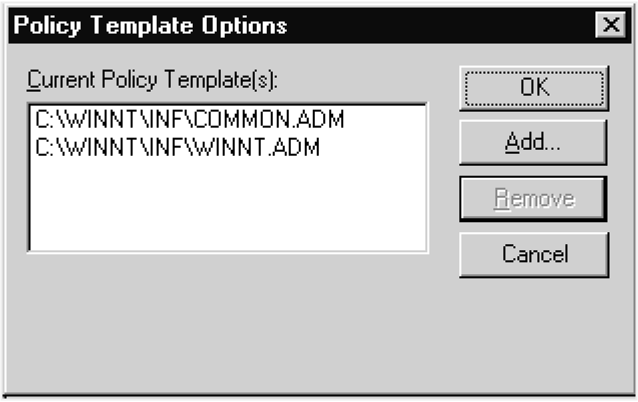
System Policy Editor Main Window

5. On the menu bar, click **Options**. The system displays a drop-down menu:



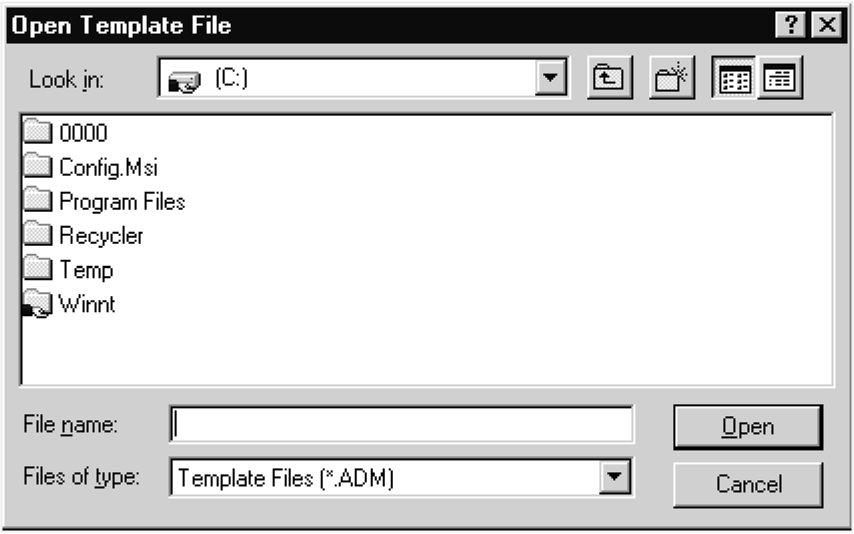
Options Drop-down Menu

6. Click **Policy Template**. The system displays the **Policy Template Options** dialog box:



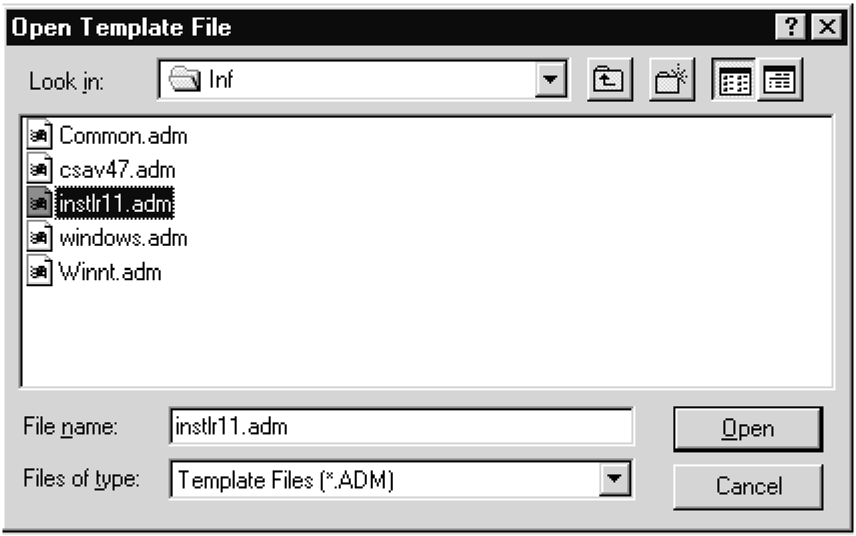
Policy Template Options Dialog Box

7. Click **Add.** The system displays the **Open Template File** dialog box:



Open Template File Dialog Box

8. Browse to the **C:\Winnt\inf** folder.

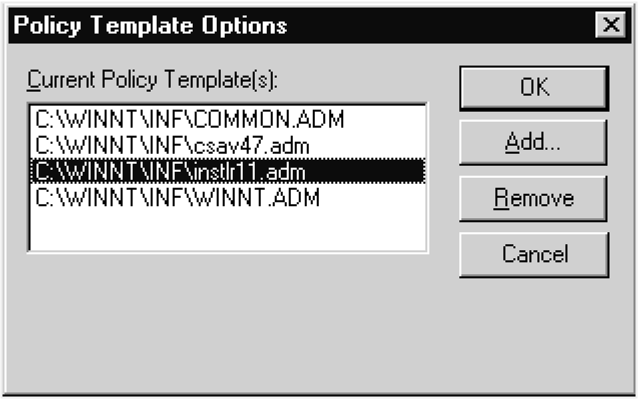


File name: instlr11.adm

Files of type: Template Files (*.ADM)

Open Template File Dialog Box – Inf\Winnt Folder

9. Select **INSTLR11.ADM**, and click **Open**. The system returns to the **Policy Template Options** dialog box. The **INSTLR11.ADM** file is now added to the **Current Policy Templates** list:

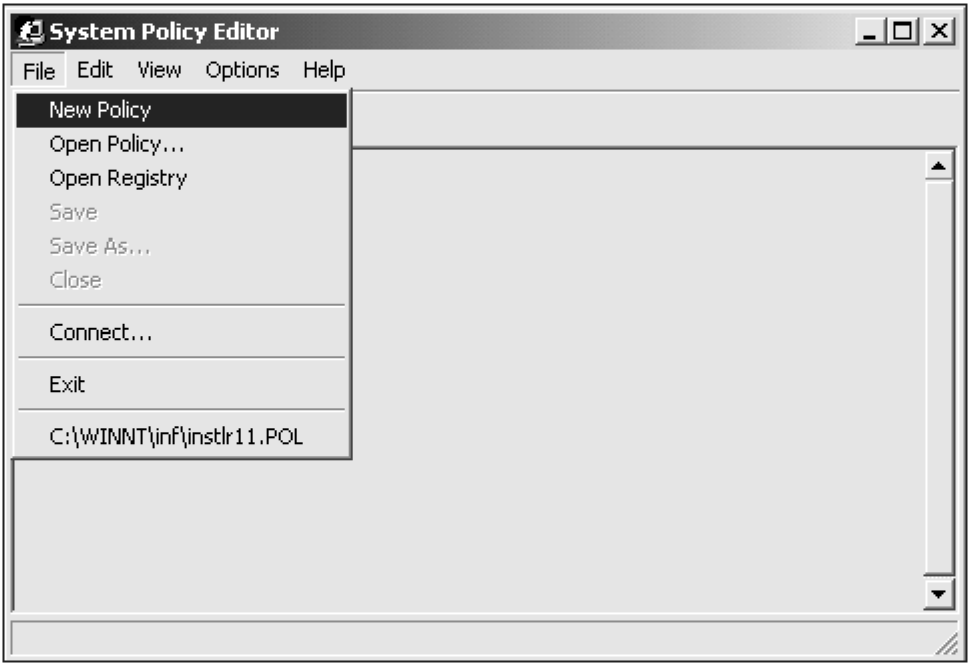


Current Policy Template(s):

C:\WINNT\INF\COMMON.ADM
C:\WINNT\INF\csav47.adm
C:\WINNT\INF\instlr11.adm
C:\WINNT\INF\WINNT.ADM

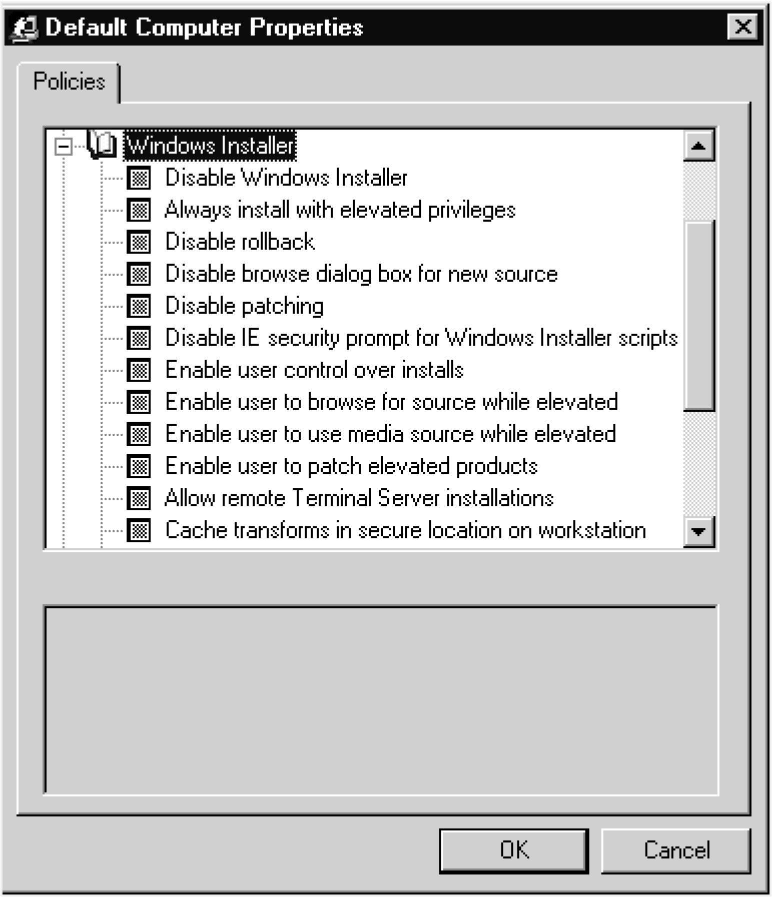
Current Policy Templates – INSTLR11.ADM Added

10. Click **OK**. The system returns to the System Policy Editor.
11. On the menu bar, click **File**. The system displays the drop-down menu:



File Drop-down Menu

12. Click **New Policy**. The system displays the **Default Computer** and **Default User** icons.
13. Double-click the **Default Computer** icon. The system displays the **Default Computer Properties** dialog box.
14. Locate Windows Installer, and click the plus sign (**+**) to expand the folder. The settings are displayed with a check box to the right of the setting:



Default Computer Properties

Windows Installer

- ▨ Disable Windows Installer
- ▨ Always install with elevated privileges
- ▨ Disable rollback
- ▨ Disable browse dialog box for new source
- ▨ Disable patching
- ▨ Disable IE security prompt for Windows Installer scripts
- ▨ Enable user control over installs
- ▨ Enable user to browse for source while elevated
- ▨ Enable user to use media source while elevated
- ▨ Enable user to patch elevated products
- ▨ Allow remote Terminal Server installations
- ▨ Cache transforms in secure location on workstation

Default Computers Properties Dialog Box

15. Select the check boxes of the settings that you want to apply, and click **OK**. The system returns to the System Policy Editor.

16. On the menu bar, click **File**, and then **Save As**. The system displays the **Save As** dialog box.
17. In the **Save in** list, browse to the:
    - **If using an NT server** – **Netlogon** folder of the Primary Domain Controller.
    - **If using a Novell® server** – **Public** folder of the preferred server.
18. In the **File name** text box, type the name of the policy, for example,
    - **In Windows 95/98/Me** – CONFIG.POL
    - **In Windows NT** – NTCONFIG.POL
19. Click **Save**.

SYSTEM POLICY TEMPLATE FOR COMMAND ANTIVIRUS

The System Policy Template for Command AntiVirus (**CSAV47.ADM**) allows you to set the Command AntiVirus installation policies for computers on the network before you install Command AntiVirus. Once you have added the template to Group Policy in Windows 2000 and Windows XP or System Policy in Windows 95/98/Me and Windows NT, you can open the template to configure the installation settings for the items on the Command AntiVirus **Preferences** menu. For more information, refer to **Using the Preferences Menu** in the ***Using Command AntiVirus*** chapter of this administrator’s guide.

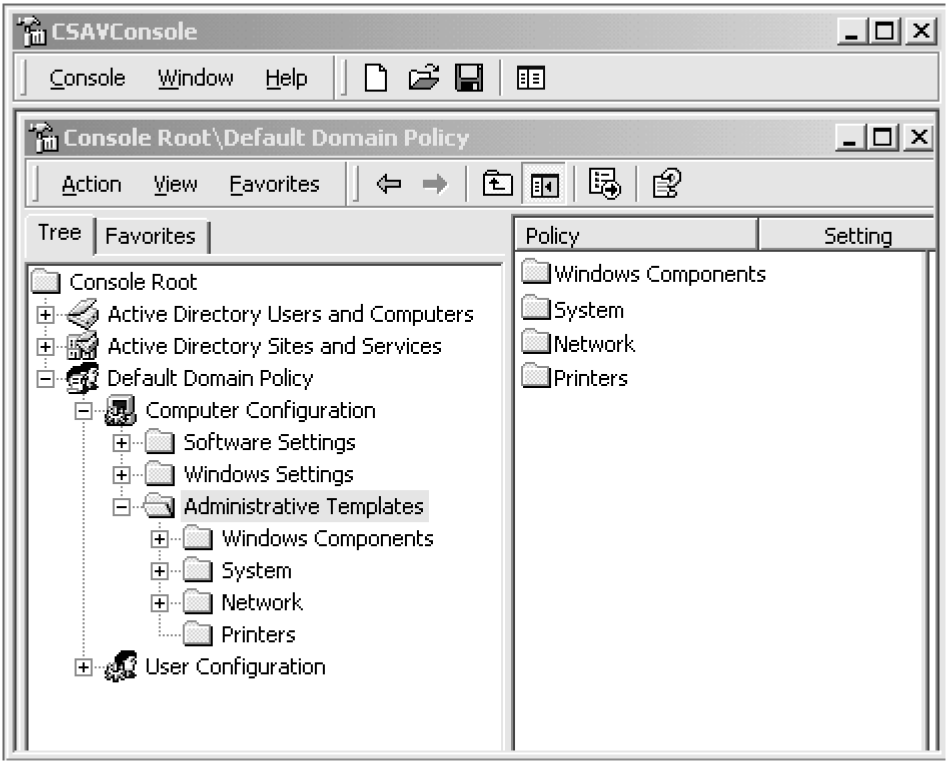
Using Group Policy

To add the template to the **Computer Configuration/Administrative Templates** folder in Group Policy and customize the Command AntiVirus settings, follow these steps:

NOTE: If you have not created a **Microsoft Management Console** file, you can access the **Computer Configuration/Administrative Templates** by running **gpedit.msc**.

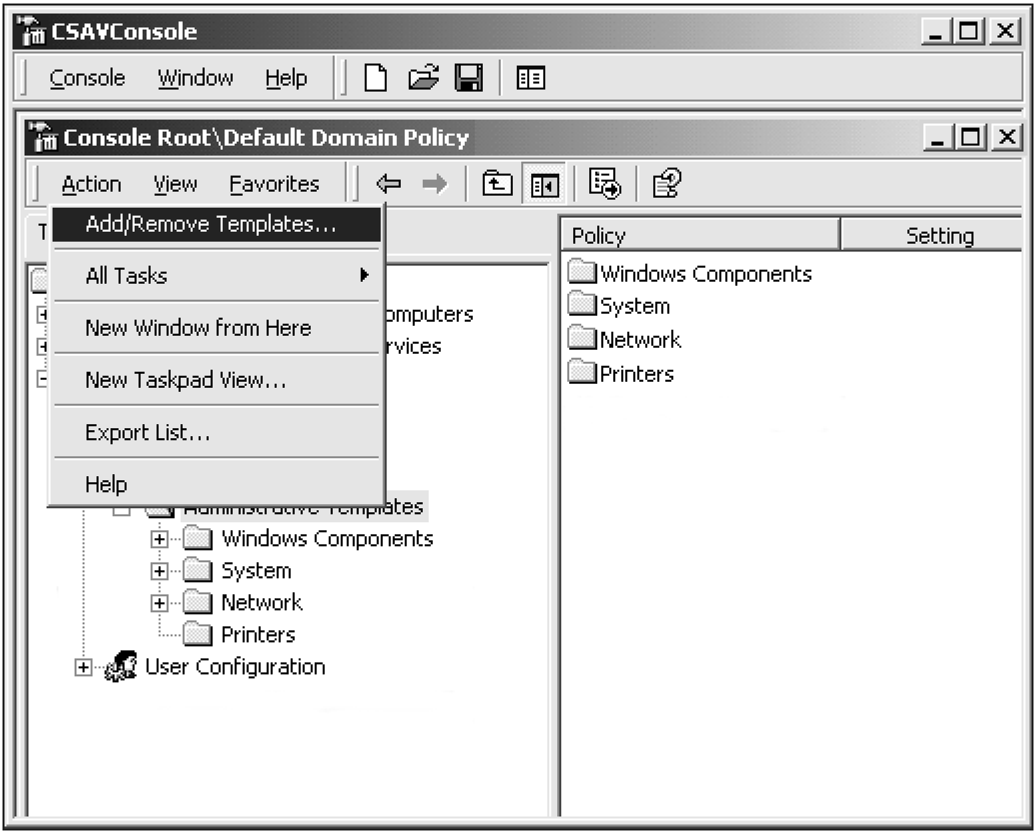
For more information on creating a Microsoft Management Console file, refer to **Configuring Group Policies** in the ***Network Administration*** chapter of this administrator’s guide.

1. Click the **Start** button on the Windows task bar.
2. Click **Run**.
3. In the text box, type **mmc.**
4. Click **OK**. The system displays the **Microsoft Management Console.**
5. In the **Console Root Tree** of the **Microsoft Management Console**, click the plus sign (**+**) to the left of the Group Policy object that you selected for Command AntiVirus, for example, **Default Domain Policy**. This action expands this item. Then, expand **Computer Configuration** and **Administrative Templates**:



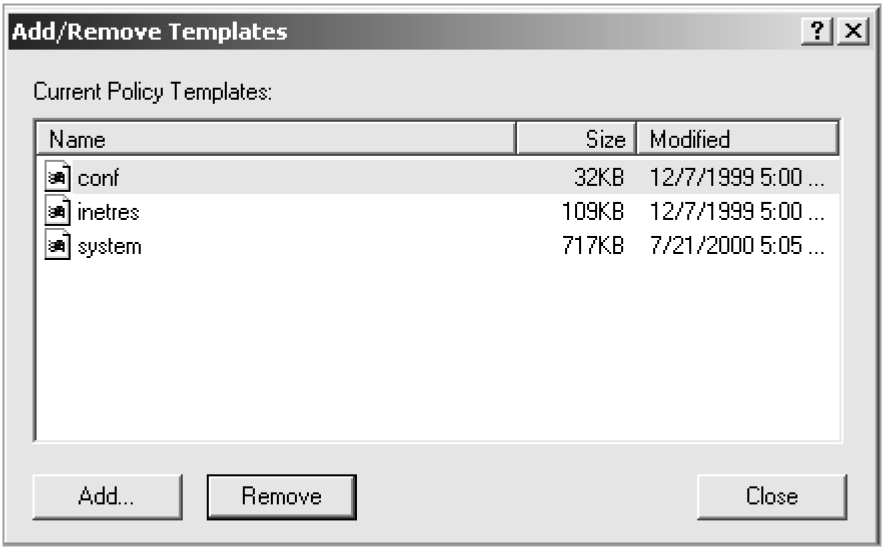
Microsoft Management Console – Administrative Templates

6. Select **Administrative Templates**.
7. On the menu bar, click **Action**. The system displays a drop-down menu:



Action Drop-down Menu

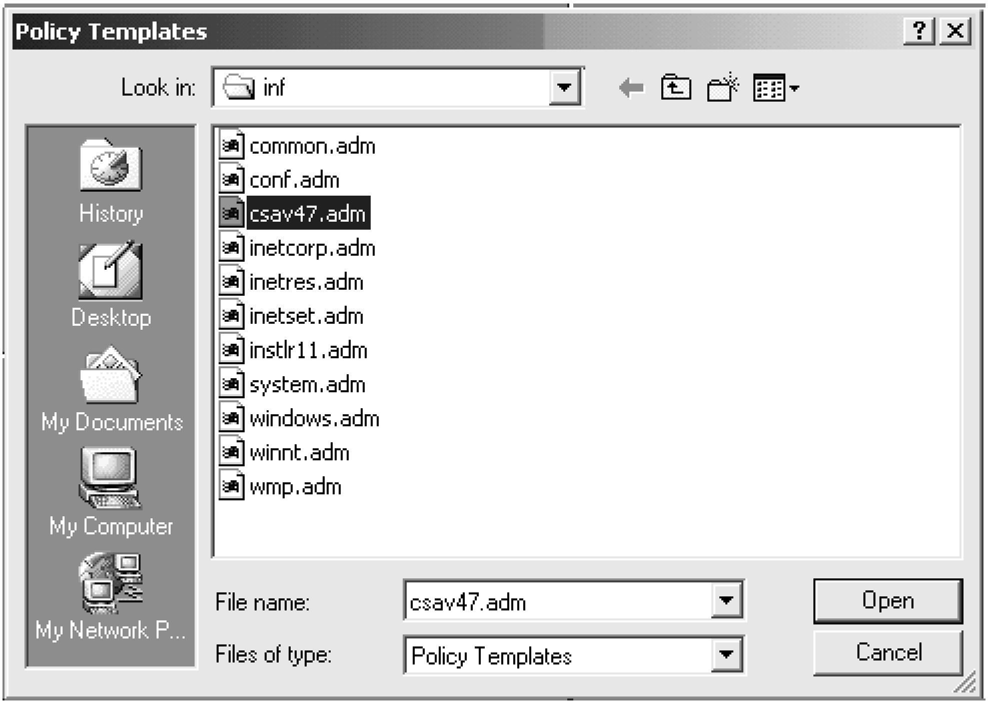
8. Click **Add/Remove Templates**. The system displays the **Add/Remove Templates dialog** box:



Name	Size	Modified
conf	32KB	12/7/1999 5:00 ...
inetres	109KB	12/7/1999 5:00 ...
system	717KB	7/21/2000 5:05 ...

Add/Remove Templates Dialog Box

9. Click the **Add** button. The system displays the **Policy Templates** dialog box:



Policy Templates

Look in: inf

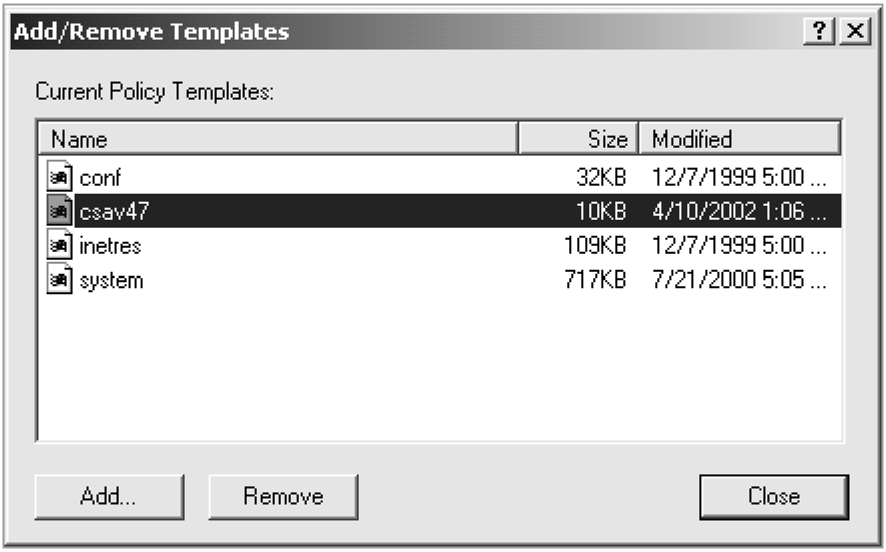
common.adm
conf.adm
csav47.adm
inetcorp.adm
inetres.adm
inetset.adm
instlr11.adm
system.adm
windows.adm
winnt.adm
wmp.adm

File name: csav47.adm

Files of type: Policy Templates

Policy Templates Dialog Box

10. Select **CSAV47.ADM**, and click **Open.** The system returns to the **Add/Remove Templates** dialog box. The **CSAV47.ADM** file is now added to the **Current Policy Templates** list:



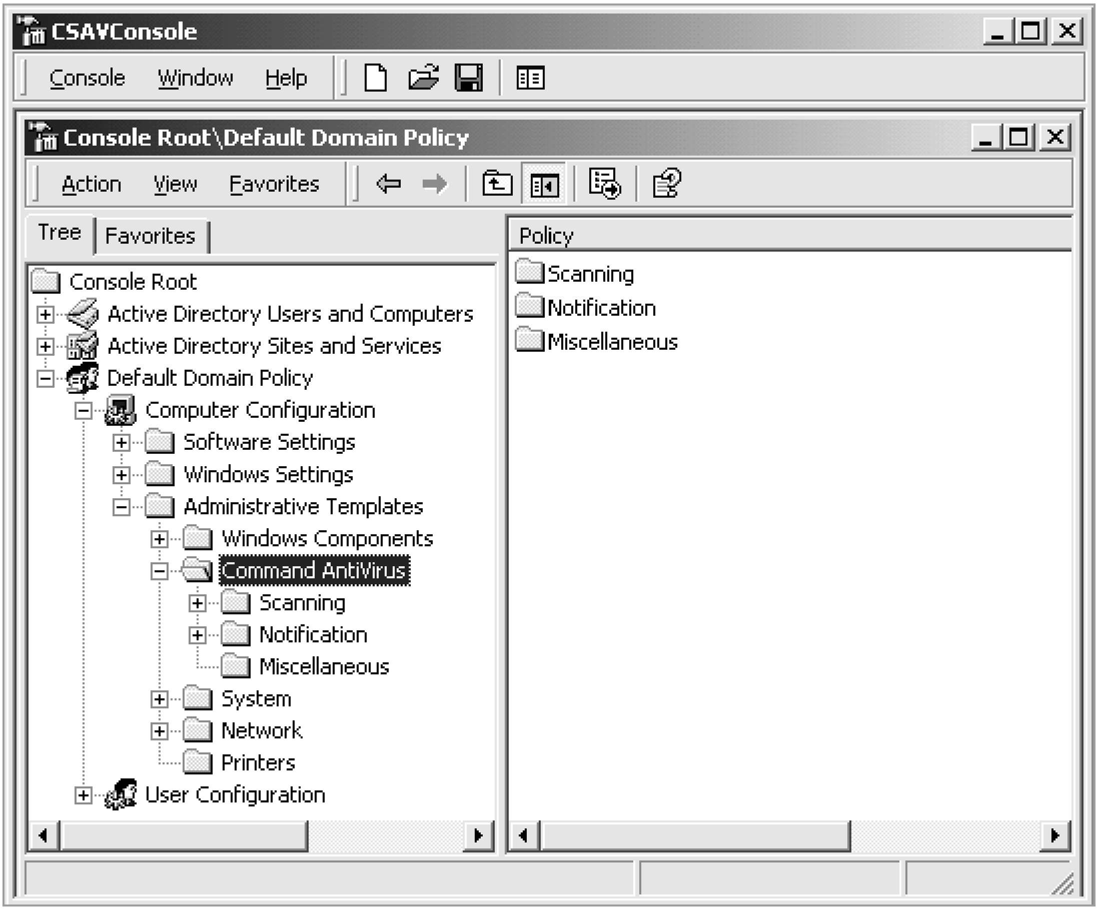
Current Policy Templates:

Name	Size	Modified
conf	32KB	12/7/1999 5:00 ...
csav47	10KB	4/10/2002 1:06 ...
inetres	109KB	12/7/1999 5:00 ...
system	717KB	7/21/2000 5:05 ...

Add/Remove Templates Dialog Box – CSAV Added

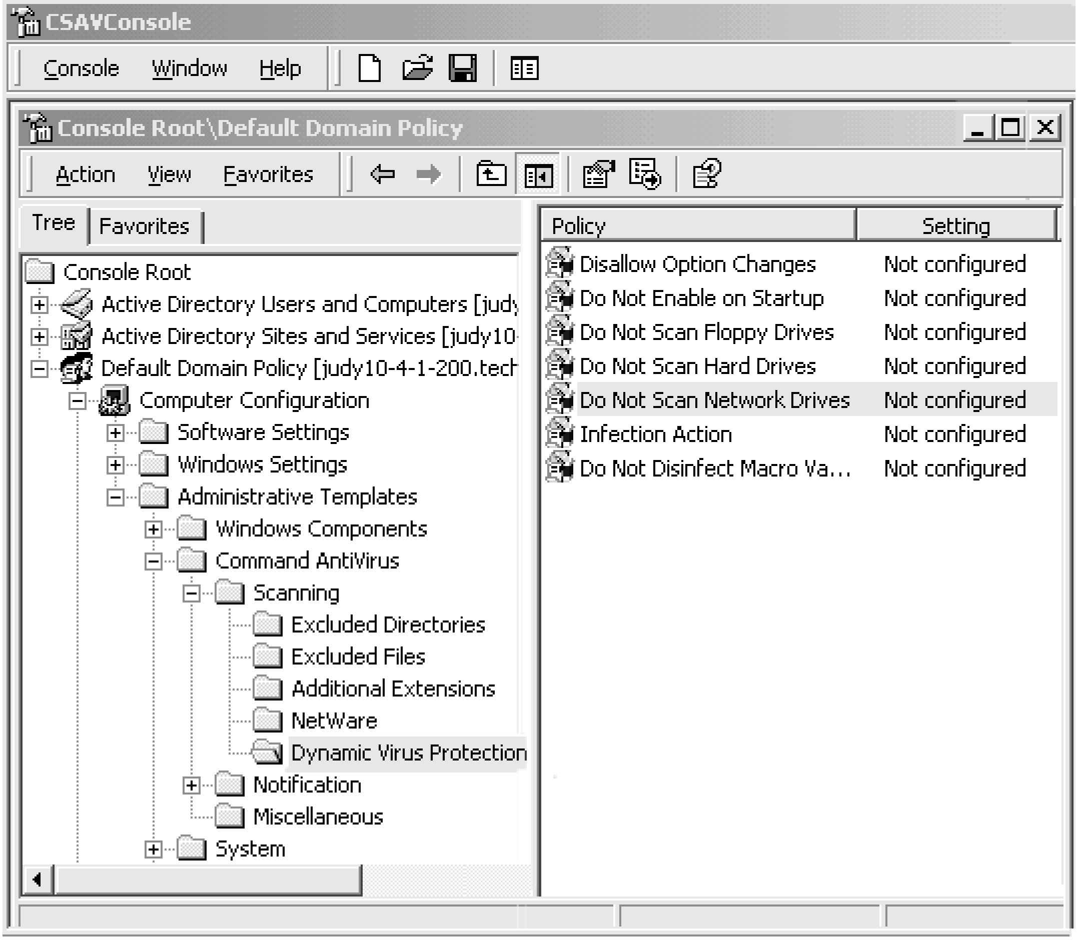
11. Click **Close**. The systems returns to the **Microsoft Management Console**. The **Command AntiVirus** folder is now added to the **Computer Configuration/ Administrative Templates** folder.

12. Click the plus sign (**+**) to the left of **Command AntiVirus** to expand the folder:



Administrative Templates – Command AntiVirus

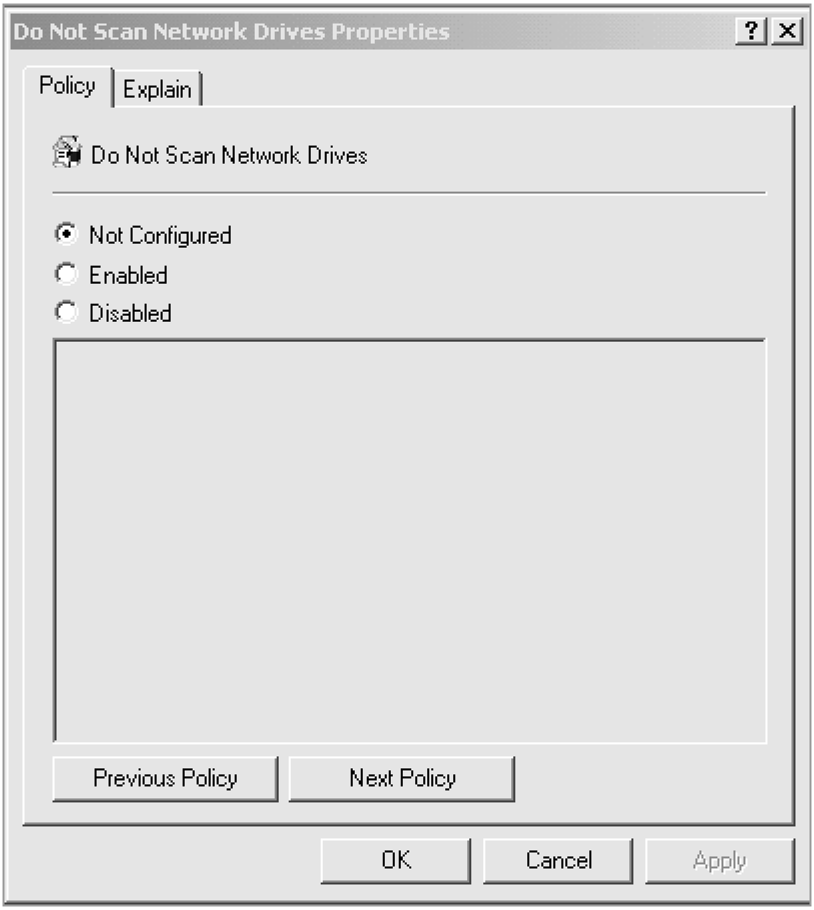
13. Expand **Scanning**, and select a **Preference**, for example, **Dynamic Virus Protection**. The settings for **Dynamic Virus Protection** are displayed in the right-hand pane. The right-hand pane also shows the present **Status** of each setting, for example, **Configured** or **Not configured**.



Policy	Setting
Disallow Option Changes	Not configured
Do Not Enable on Startup	Not configured
Do Not Scan Floppy Drives	Not configured
Do Not Scan Hard Drives	Not configured
Do Not Scan Network Drives	Not configured
Infection Action	Not configured
Do Not Disinfect Macro Va...	Not configured

Dynamic Virus Protection – Do Not Scan Network Drives

14. Double-click a setting, for example, **Do Not Scan Network Drives**, to configure it. The system displays the **Do Not Scan Network Drives Properties** dialog box:



Do Not Scan Network Drives Properties

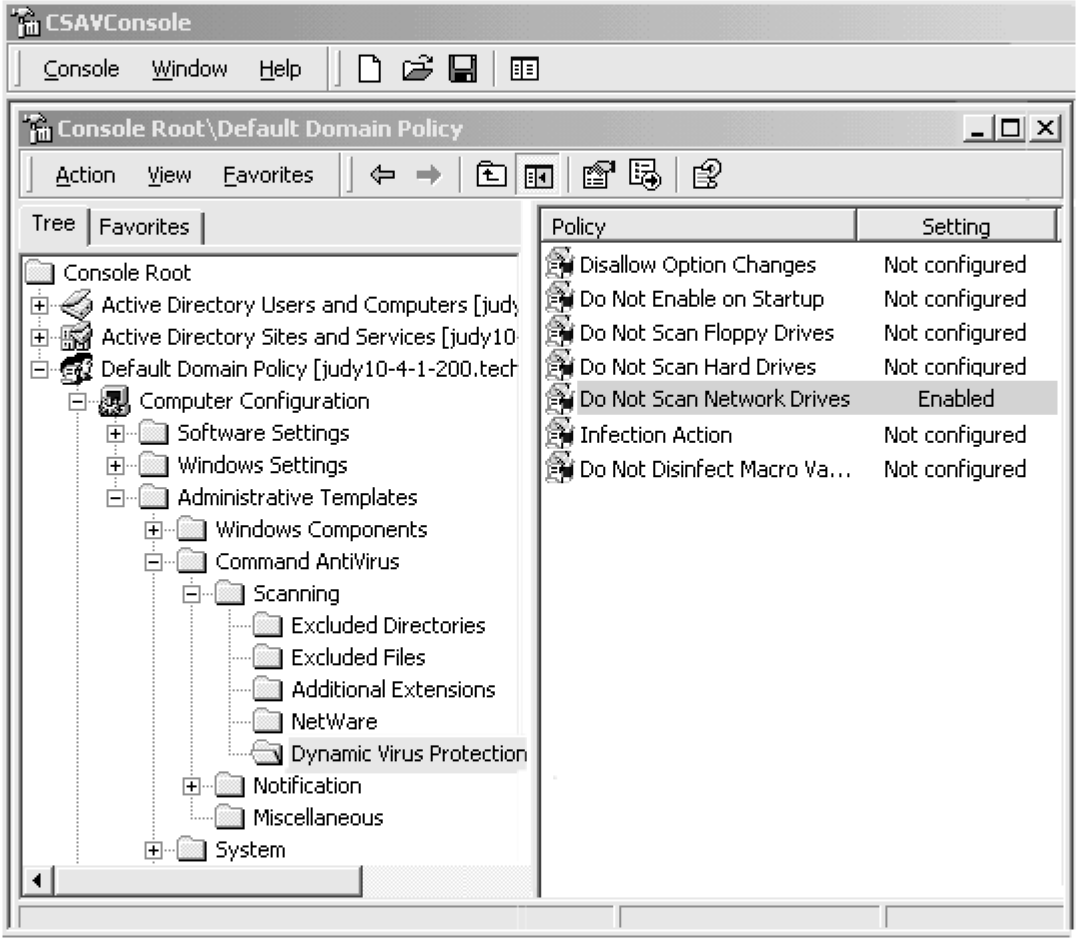
Do Not Scan Network Drives

● Not Configured
○ Enabled
○ Disabled

Do Not Scan Network Drives Properties Dialog Box

15. Select **Enabled**, and click **OK**. The system returns to the **Microsoft Management Console**. **Do Not Scan Network Drives** is now **Enabled**.

NOTE: You can also use the **Previous Policy** and **Next Policy** buttons to configure other settings. The setting that you have just configured is saved by default.



- Console Root
  - Active Directory Users and Computers [judy
  - Active Directory Sites and Services [judy10-
  - Default Domain Policy [judy10-4-1-200.tech
    - Computer Configuration
      - Software Settings
      - Windows Settings
      - Administrative Templates
        - Windows Components
        - Command AntiVirus
          - Scanning
            - Excluded Directories
            - Excluded Files
            - Additional Extensions
            - NetWare
            - Dynamic Virus Protection
          - Notification
          - Miscellaneous
        - System

Policy	Setting
Disallow Option Changes	Not configured
Do Not Enable on Startup	Not configured
Do Not Scan Floppy Drives	Not configured
Do Not Scan Hard Drives	Not configured
Do Not Scan Network Drives	Enabled
Infection Action	Not configured
Do Not Disinfect Macro Va...	Not configured

Dynamic Virus Protection – Do Not Scan Network Drives Enabled

16. Repeat Steps **13** through **15** for each **Preference** and setting that you want to customize.

Using System Policy

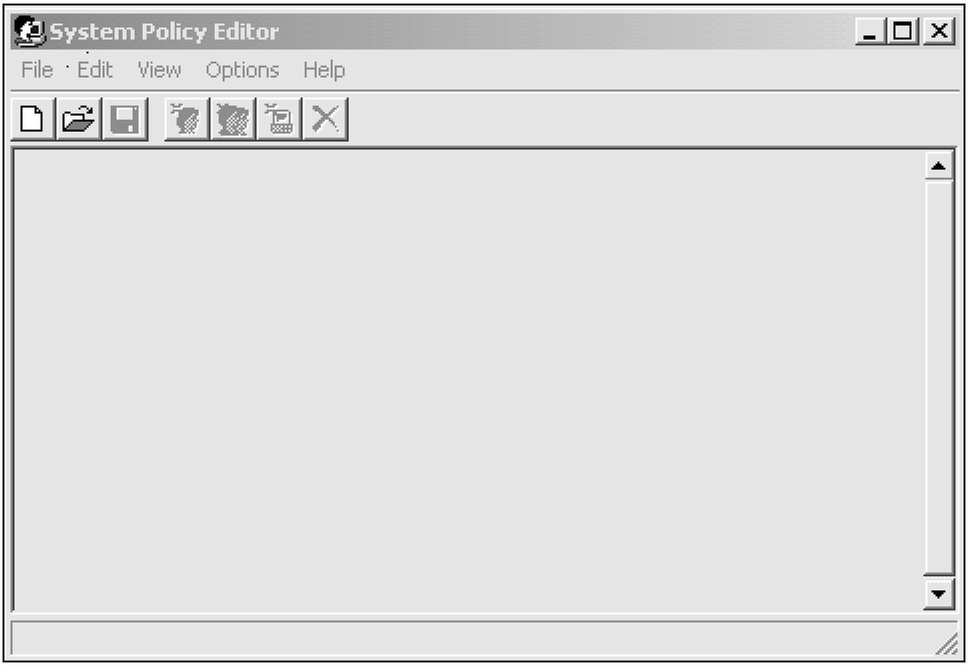
95/98/Me

To use this template on Windows 95/98/Me, you must have SYSPOL and POLEDIT installed.

9x/Me/NT

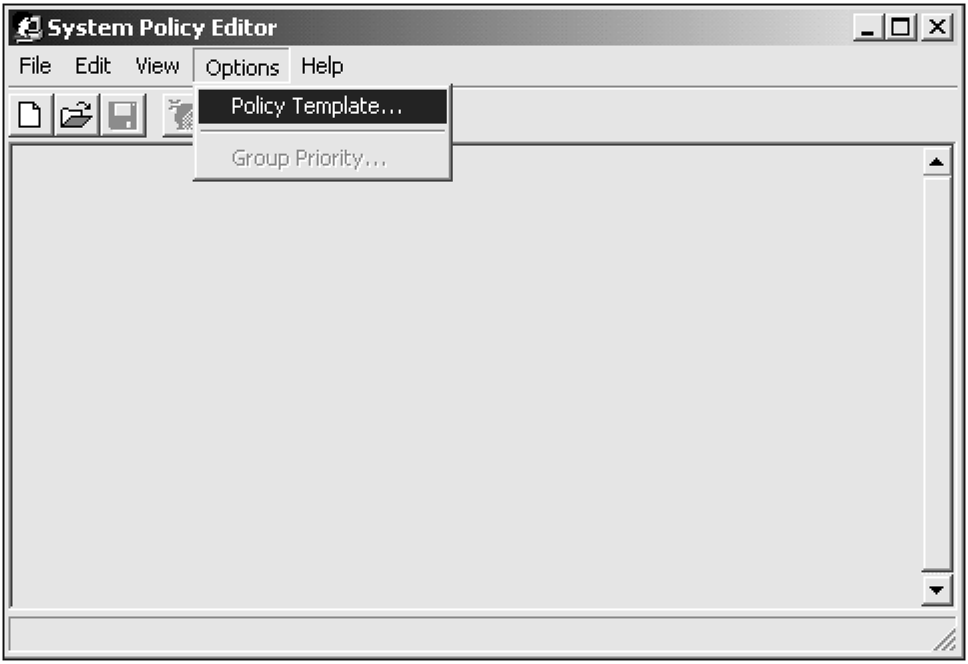
To add the template to System Policy and customize the Command AntiVirus settings, follow these steps:

1. Click the **Start** button on the Windows task bar.
2. Click **Run**.
3. In the text box, type **poledit**.
4. Click **OK**. The system displays the System Policy Editor:



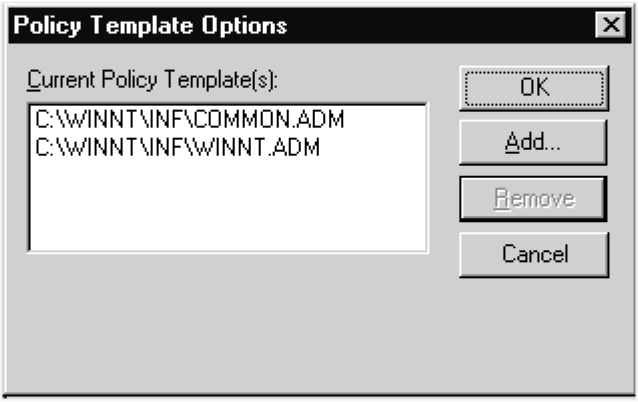
System Policy Editor Main Window

5. On the menu bar, click **Options**. The system displays a drop-down menu:



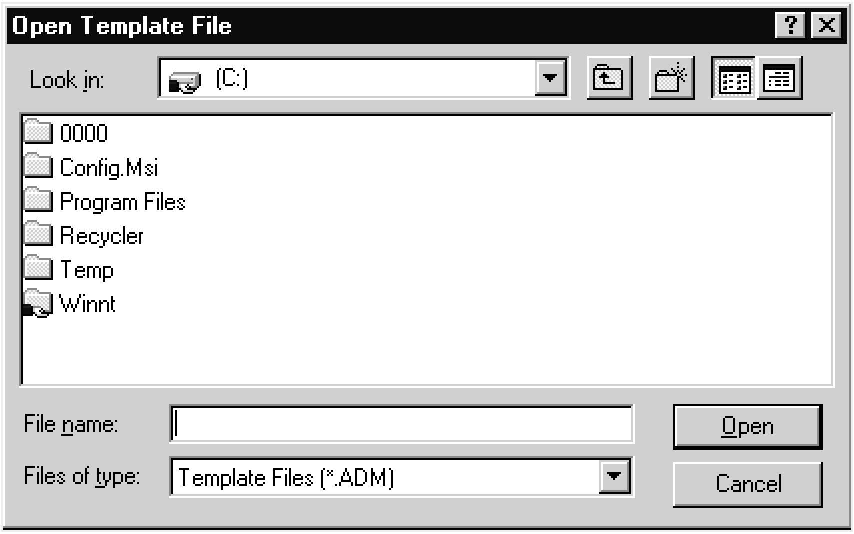
Options Drop-down Menu

6. Click **Policy Template**. The system displays the **Policy Template Options** dialog box:



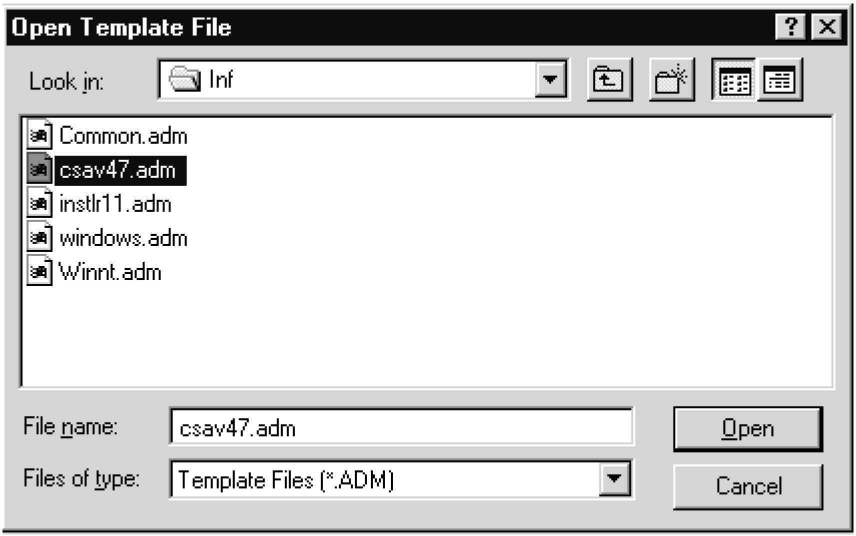
Policy Template Options Dialog Box

7. Click **Add**. The system displays the **Open Template File** dialog box:



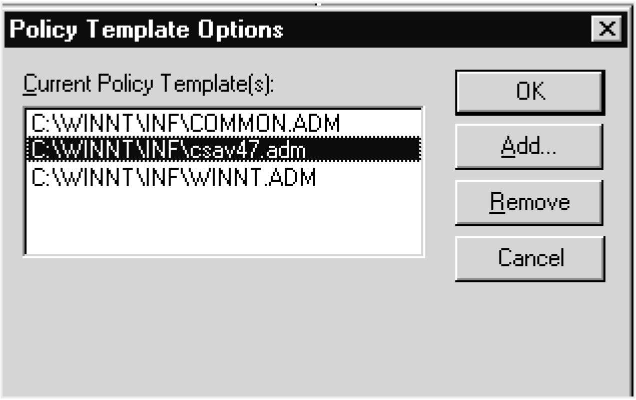
Open Template File Dialog Box

8. Browse to the **C:\Winnt\inf** folder:



Open Template File Dialog Box – Inf\CSAV47 Folder

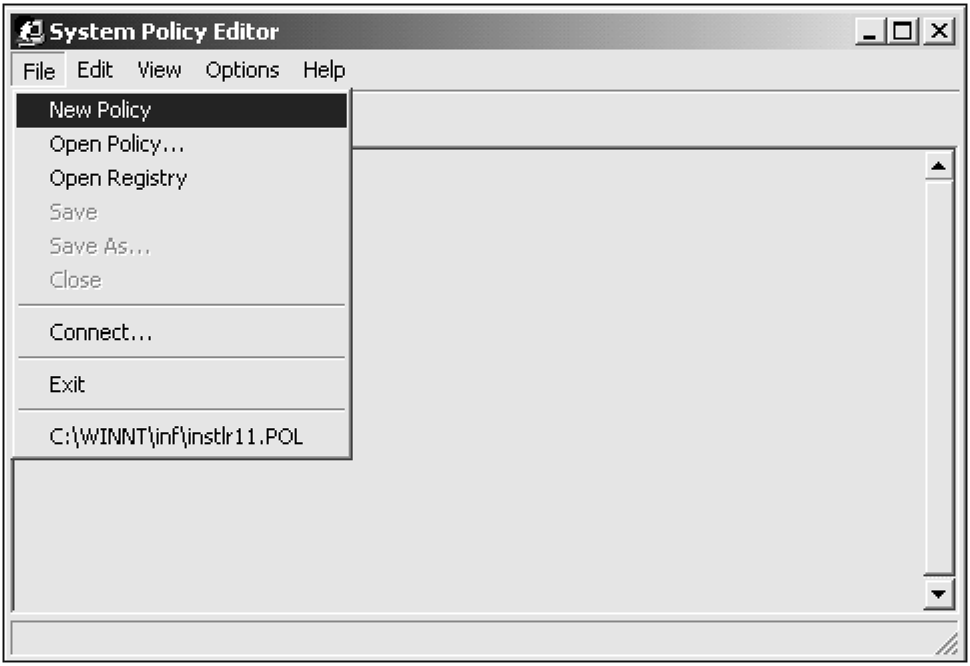
9. Select **CSAV47.ADM**, and click **Open.** The system returns to the **Policy Template Options** dialog box. The **CSAV47.ADM** file is now added to the **Current Policy Templates** list:



C:\WINNT\INF\COMMON.ADM
C:\WINNT\INF\csav47.adm
C:\WINNT\INF\WINNT.ADM

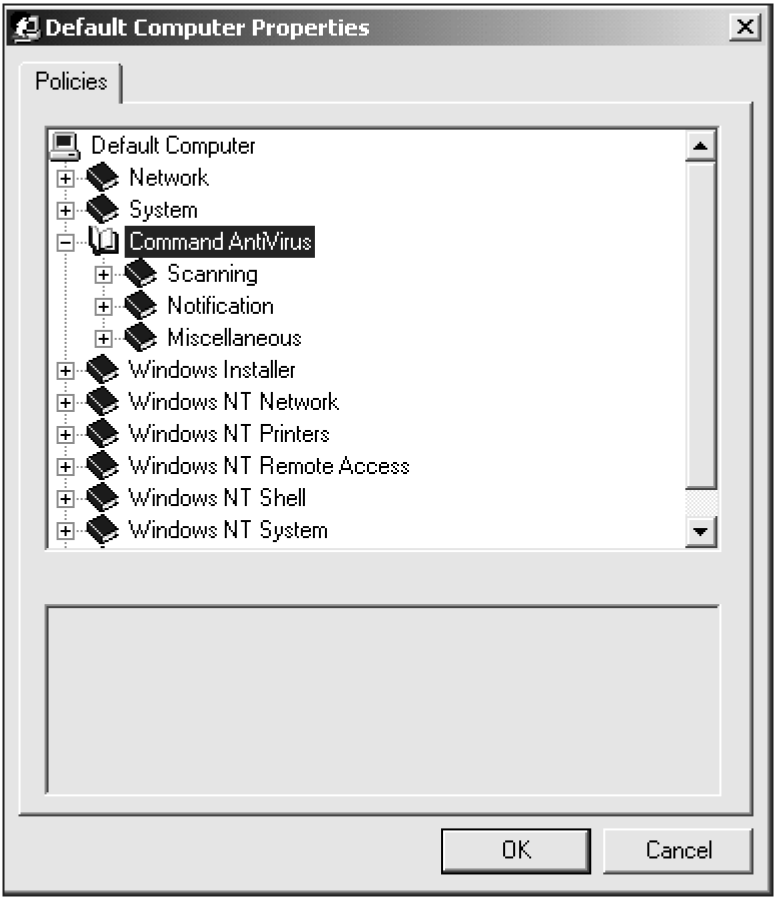
Current Policy Templates List – CSAV47.ADM Added

10. Click **OK**. The system returns to the System Policy Editor.
11. On the menu bar, click **File**. The system displays the drop-down menu:



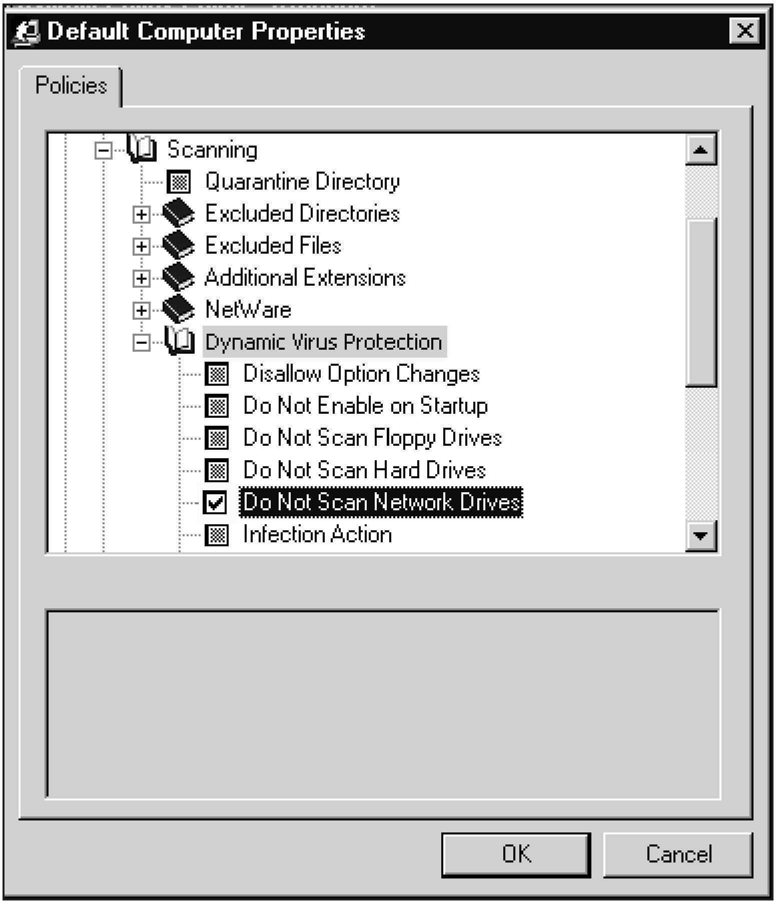
File Drop-down Menu

12. Click **New Policy**. The system displays the **Default Computer** and **Default User** icons.
13. Double-click the **Default Computer** icon. The system displays the **Default Computer Properties** dialog box.
14. Locate **Command AntiVirus**, and click the plus sign to expand the folder:



Default Computer Properties Dialog Box

15. Expand **Scanning**, and expand a **Preference**, for example, **Dynamic Virus Protection** (**DVP**). The settings for **Dynamic Virus Protection** are displayed with a check box to the left of the setting.



Default Computer Properties

Policies

- ⊟ Scanning
  - ▨ Quarantine Directory
  - ⊞ Excluded Directories
  - ⊞ Excluded Files
  - ⊞ Additional Extensions
  - ⊞ NetWare
  - ⊟ Dynamic Virus Protection
    - ▨ Disallow Option Changes
    - ▨ Do Not Enable on Startup
    - ▨ Do Not Scan Floppy Drives
    - ▨ Do Not Scan Hard Drives
    - ☑ Do Not Scan Network Drives
    - ▨ Infection Action

Default Computer Properties Dialog Box – DVP

16. Select the check boxes of the settings that you want to apply, for example, **Do Not Scan Network Drives**.
17. Repeat Steps **15** through **16** for each **Preference** that you want to customize.
18. Click **OK.** The system returns to the System Policy Editor.

19. On the menu bar, click **File**, and then **Save As**. The system displays the **Save As** dialog box.
20. In the **File name** text box, type the name of the policy, for example, **CSAV47.POL**, and click **Save**.

CUSTOM INSTALLATION WIZARD

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

Using the wizard, you can import Command AntiVirus settings from a previous version, add or remove features, and create custom scan tasks. If you are not using the System Policy Template for Command AntiVirus, you can also use the wizard to customize the Command AntiVirus settings.

The wizard uses the Command AntiVirus Windows Installer package (MSI file) to create a custom Windows installer transform (MST file) that contains your customized installation features and settings. You can then deploy the MST file with the Command AntiVirus installation MSI file to computers throughout the network.

NOTE: You can use the wizard to create a new MST file or to modify an existing file. No changes are made to the Command AntiVirus MSI file.

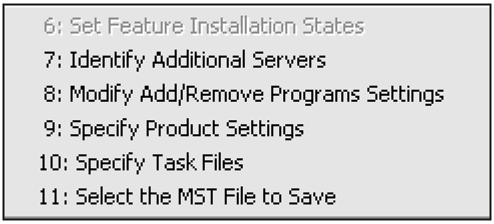
The Custom Installation Wizard for Command AntiVirus contains the following customization options:

- **Set Feature Installation States** – Allows you to select the features that you want to install and how they will be installed. You can also select whether the feature is displayed or hidden during the installation process and when the user is adding or removing features after CSAV is installed.
- **Identify Additional Servers** – Allows you to specify additional network servers that have a copy of the installation folder tree. If you install features to run from the server or to be installed when the feature is first accessed, this option ensures that there is always access to an available network server.

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

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

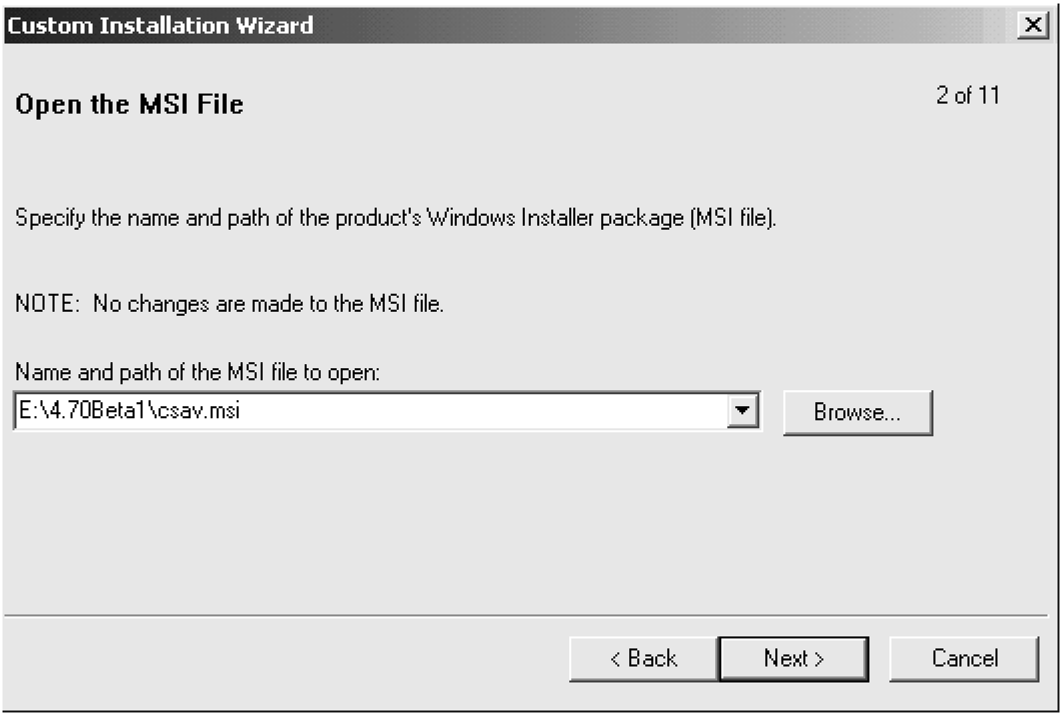
- To go back to the previous dialog box, click **Back**.
- To exit the wizard during the process, click **Cancel**.
- To save your changes to the MST file, click **Finish**.
- To exit the wizard after you have completed the process, click **Exit**.
- To go to any page in the wizard, click the down arrow to the right of the page number in the upper-right corner of the dialog box. The system displays the following drop-down list box containing the wizard page names and numbers. Just click the page that you want. This option is available starting with **Page 6**.


6: Set Feature Installation States
7: Identify Additional Servers
8: Modify Add/Remove Programs Settings
9: Specify Product Settings
10: Specify Task Files
11: Select the MST File to Save

Wizard Page Number Box

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

1. Click the **Start** button on the Windows taskbar.
2. Select **Programs**.
3. Select **COMMANDCentral**.
4. Click **Custom Installation Wizard.** The system displays the **Welcome** dialog box.
5. Click **Next.** The system displays the **Open the MSI File** dialog box:



Specify the name and path of the product's Windows Installer package (MSI file).

NOTE: No changes are made to the MSI file.

Name and path of the MSI file to open: E:\4.70Beta1\csav.msi

Open the MSI File Dialog Box

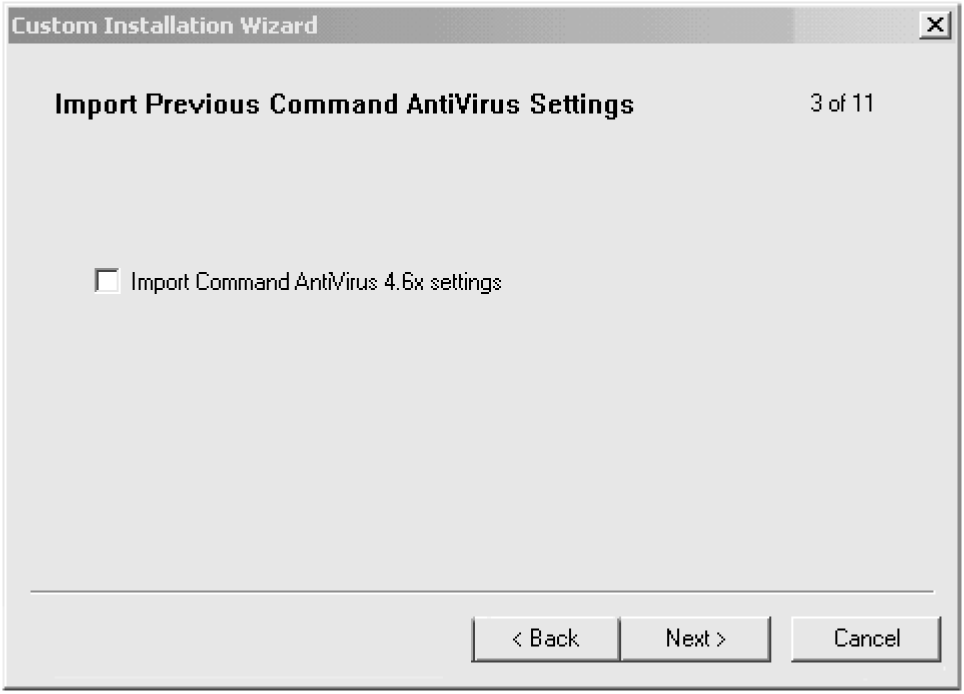
6. In the **Name and path of the MSI file to open** text box, type the path and name of the Command AntiVirus MSI file that you want to customize, for example:

```
E:\4.70BETA1\CSAV.MSI
```

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

If you are using the Custom Installation Wizard within the Command AntiVirus Deployment Prep Wizard, the path is set by default, and the text box is unavailable.

7. Click **Next**. The system displays the **Import Previous Command AntiVirus Settings** dialog box:



Custom Installation Wizard

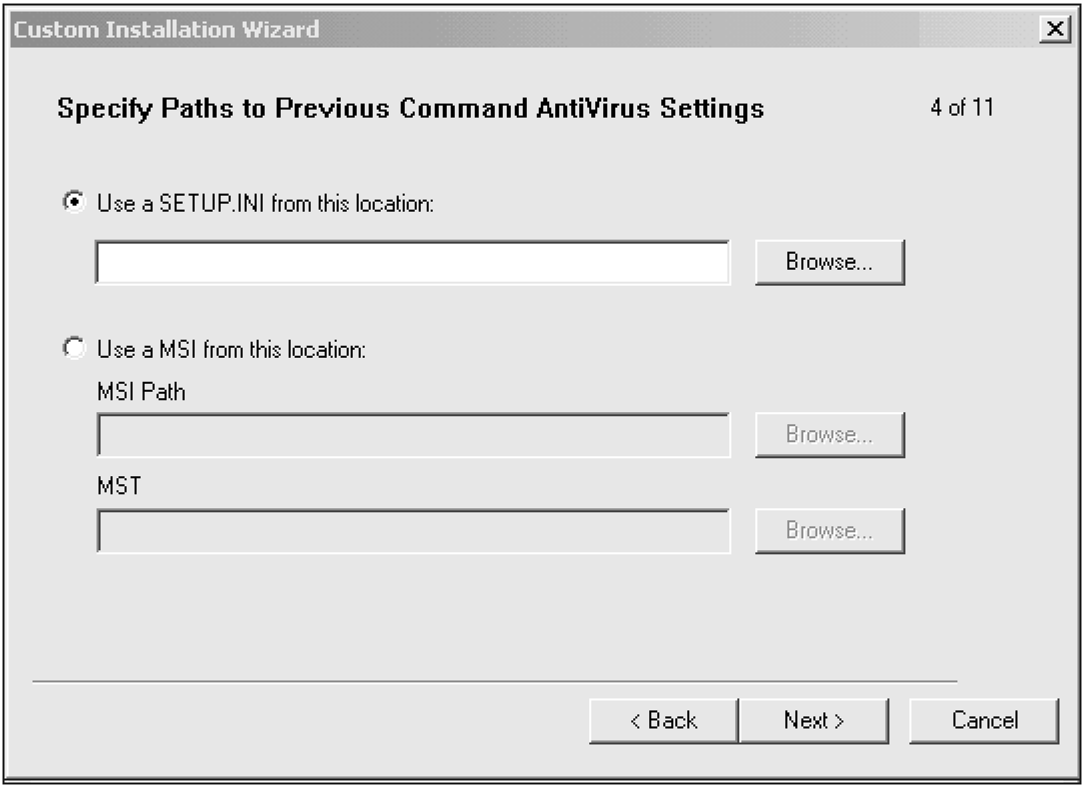
Import Previous Command AntiVirus Settings 3 of 11

☐ Import Command AntiVirus 4.6x settings

Import Previous Command AntiVirus Settings Dialog Box

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

    - If you do not want to import settings, click **Next**, and go to **Step 11**.
    - If you want to import settings from a 4.6x version of Command AntiVirus, select the **Import Command AntiVirus 4.6x settings** check box, and click **Next**. The system displays the **Specify Paths to Previous Command AntiVirus Settings** dialog box:



Specify Paths to Previous Command AntiVirus Settings

4 of 11

● Use a SETUP.INI from this location:

○ Use a MSI from this location:

MSI Path

MST

Specify Paths to Previous Command AntiVirus Settings Dialog Box

This dialog box allows you to import settings from a previously configured Command AntiVirus 4.6x **SETUP.INI** file or **MST** file.

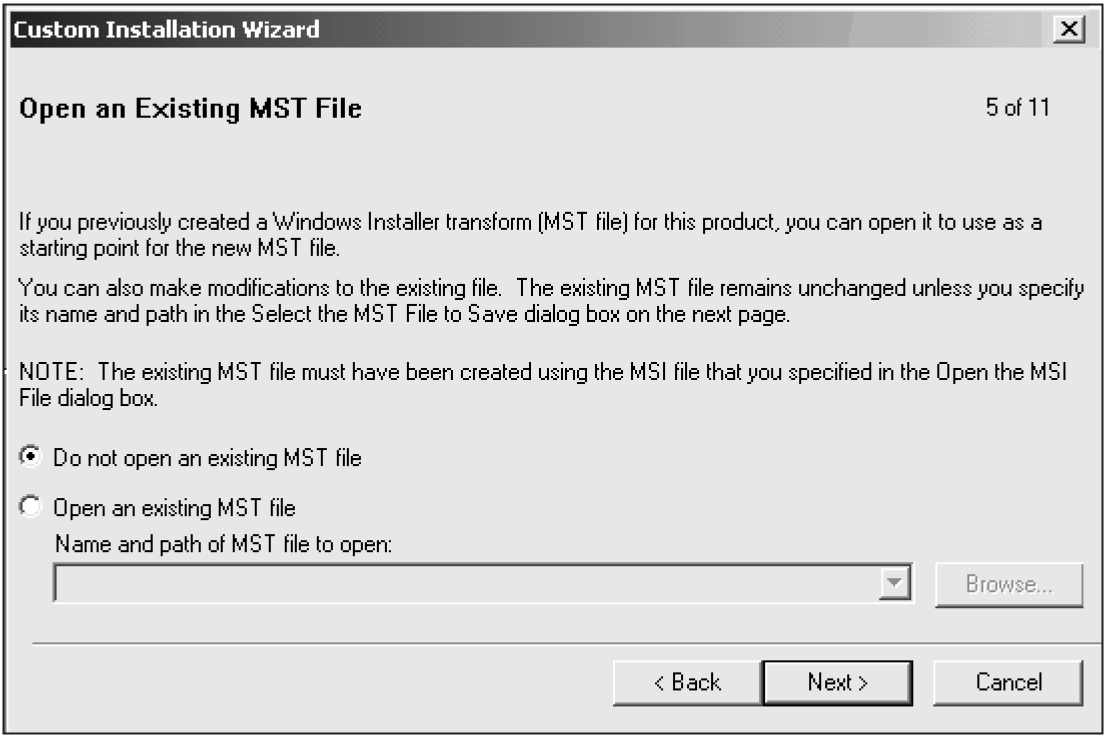
9. Select the file type you want to transfer from, for example, **Use a SETUP.INI from this location**, and in the text box, type the path to the file.

NOTE: If you selected **Use an MSI**, you need to provide the location of both the MSI and the MST files.

You can use the **Browse** button to locate the files.

10. Depending on the file type you selected in **Step 9**:

- **Use a SETUP.INI from this location** – go to **Step 12**.
- **Use an MSI** – click **Next**. The system displays the **Open an Existing MST File** dialog box:



Custom Installation Wizard

Open an Existing MST File

5 of 11

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

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

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

● Do not open an existing MST file

○ Open an existing MST file

Name and path of MST file to open:

Open an Existing MST File Dialog Box

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

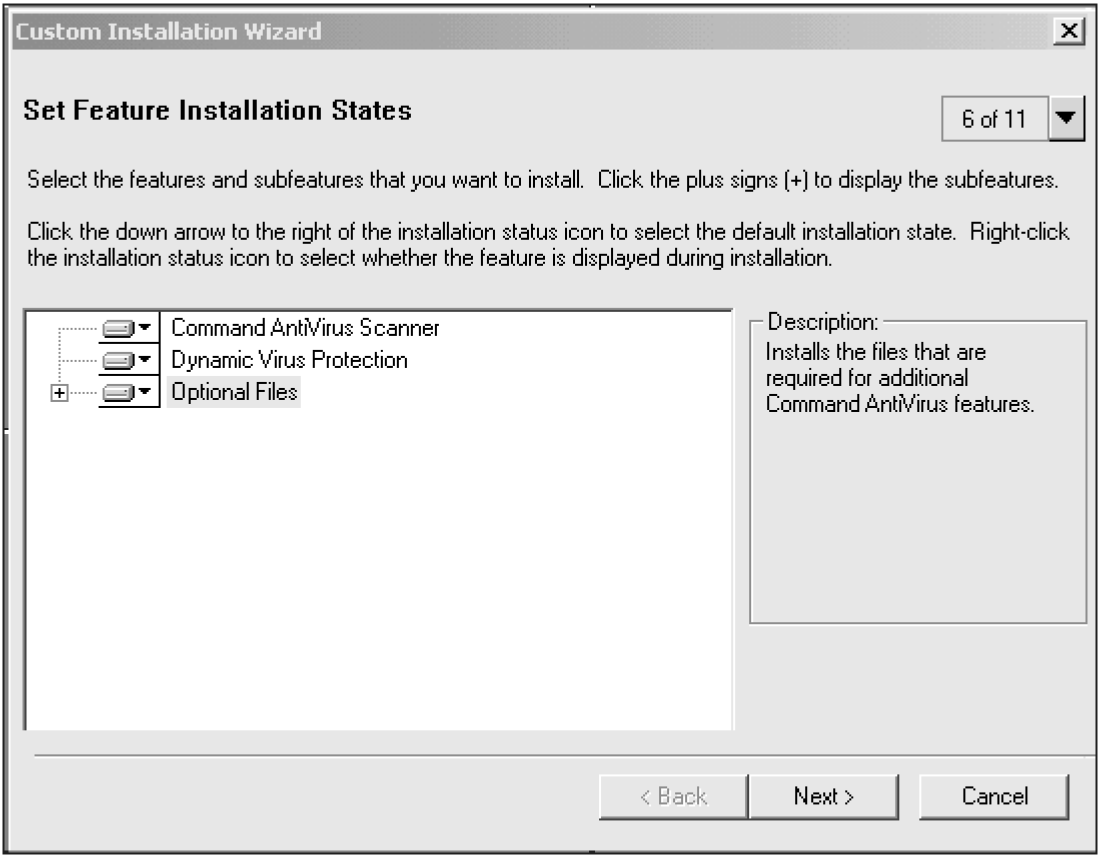
    If you have previously created a Command AntiVirus MST file, you can open the existing MST file to use as a starting point for a new file. You can also make changes to the existing file.

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

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

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

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



Custom Installation Wizard

Set Feature Installation States

6 of 11

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

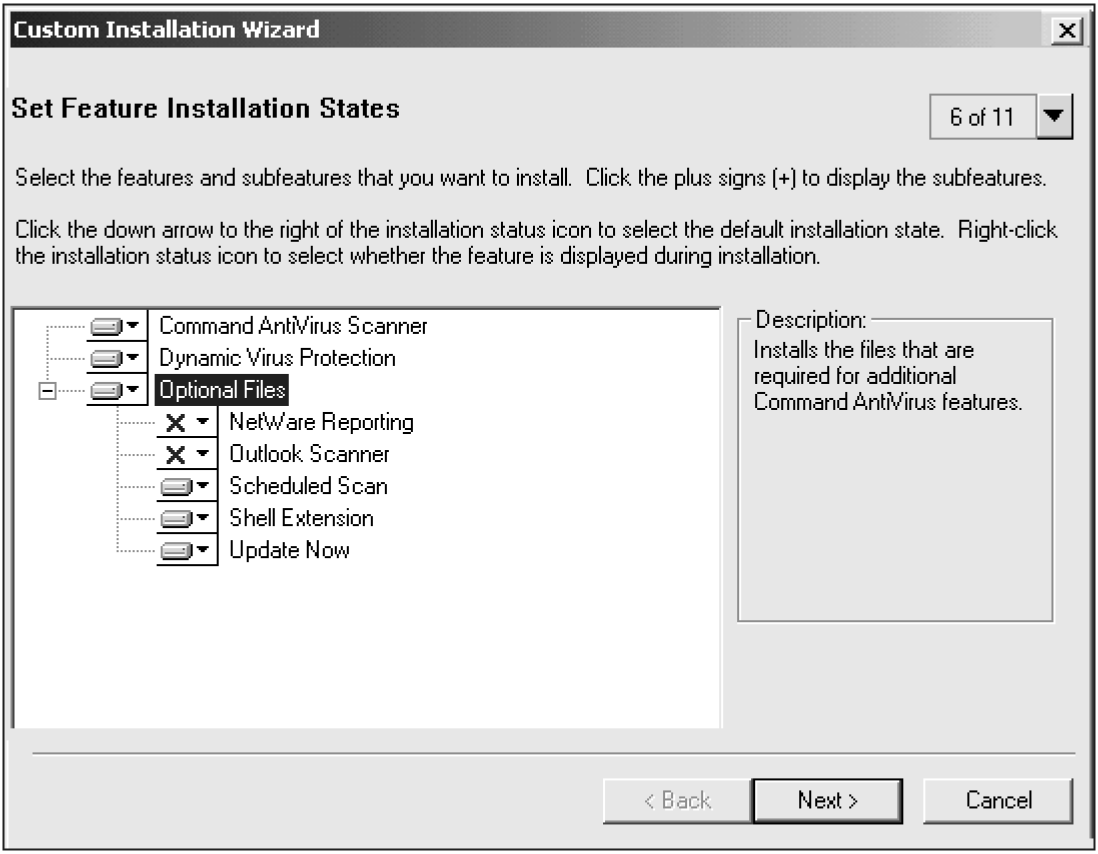
Click the down arrow to the right of the installation status icon to select the default installation state. Right-click the installation status icon to select whether the feature is displayed during installation.

- Command AntiVirus Scanner
- Dynamic Virus Protection
- Optional Files

Description:
Installs the files that are required for additional Command AntiVirus features.

Set Feature Installation States Dialog Box

13. 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.



Custom Installation Wizard

Set Feature Installation States

6 of 11

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

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

- Command AntiVirus Scanner
- Dynamic Virus Protection
- Optional Files
  - ✗ NetWare Reporting
  - ✗ Outlook Scanner
  - Scheduled Scan
  - Shell Extension
  - Update Now

Description:
Installs the files that are required for additional Command AntiVirus features.

Set Feature Installation States Dialog Box – Subfeatures Displayed

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

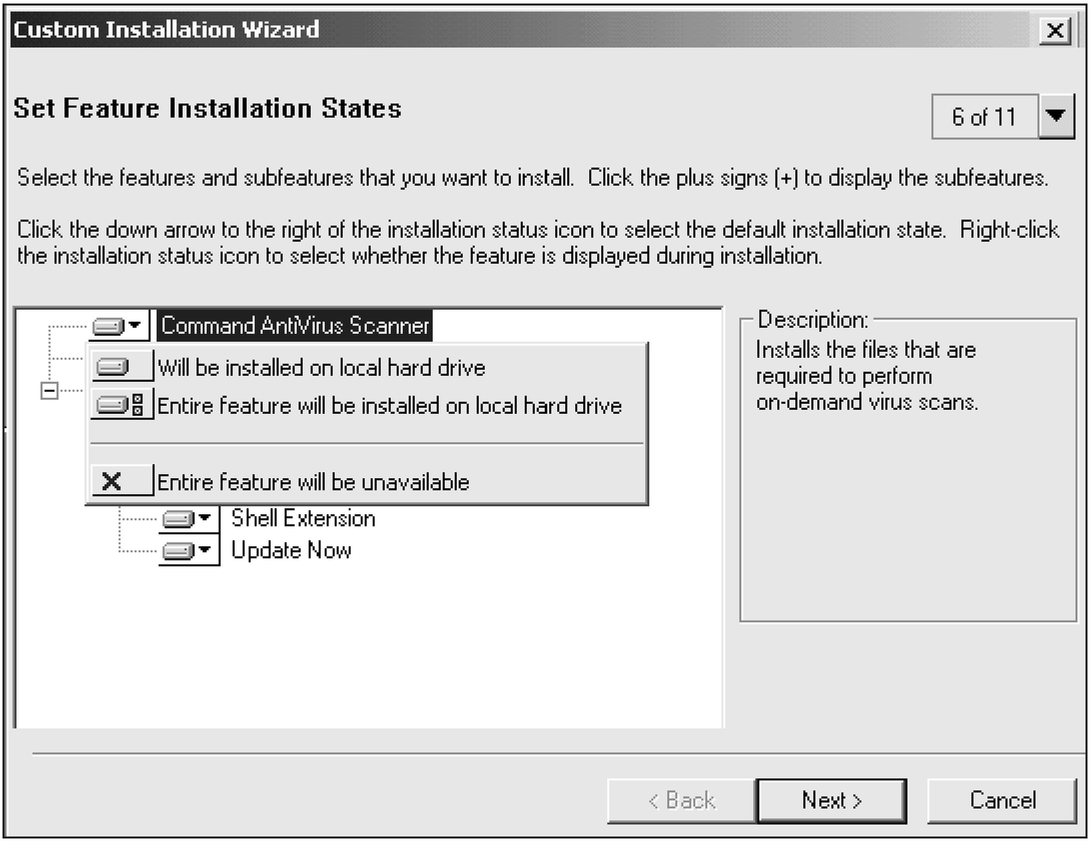
NOTE: For **NetWare Reporting** to work, the Novell® NetWare® client **must** be installed.

  - **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.
  - **Update Now** – installs the files that are required to allow the end user to update definition files, components, and full product. This subfeature is installed by default.

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



Custom Installation Wizard
Set Feature Installation States
6 of 11

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

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

Command AntiVirus Scanner
Will be installed on local hard drive
Entire feature will be installed on local hard drive
Entire feature will be unavailable
Shell Extension
Update Now
Description:

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

Set Feature Installation States Dialog Box – Drop-down Menu

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

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

Will be installed on local hard drive – installs the selected feature or subfeature on the local hard drive. If you select a subfeature, this option also installs the parent feature. For example, if you select to install the **Outlook Scanner**, the **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**, all of the subfeatures are also installed.

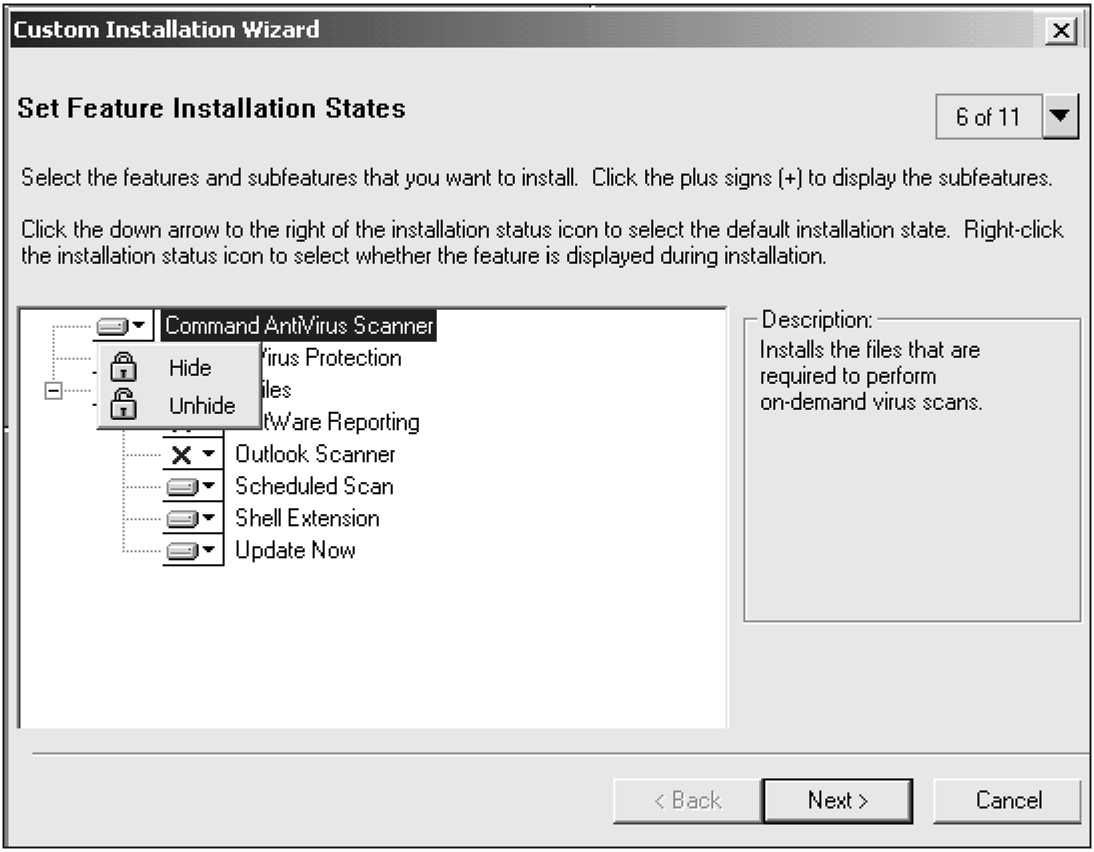
If you select a subfeature, this option installs the parent feature and the selected subfeature. For example, if you select to install **NetWare Reporting**, **Optional Files** is also installed.

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

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

You can also select whether the feature is displayed during the installation process and when the user is adding or removing features after CSAV is installed.

Right-click the down arrow to the right of the installation state icon of a feature or subfeature. The system displays a drop-down menu:



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

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

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

Set Feature Installation States Dialog Box – Hide/Unhide Drop-Down Menu

Select **one** of the following:

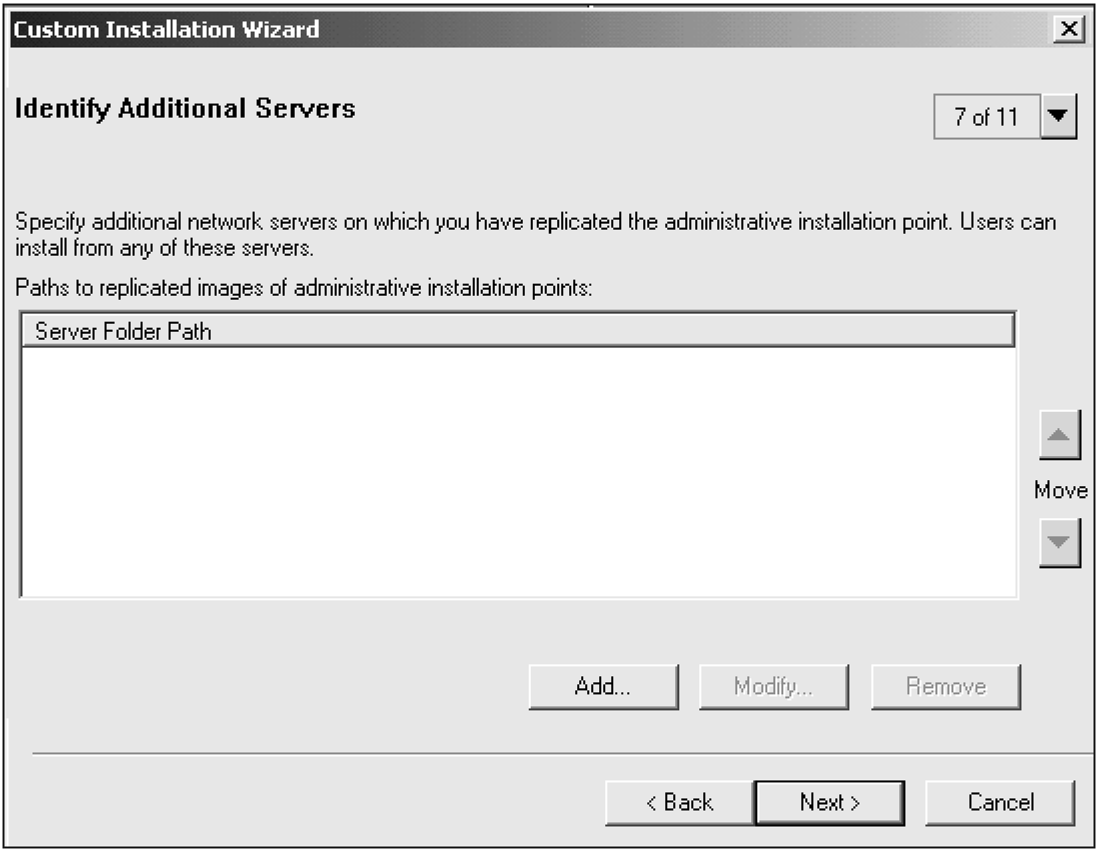
- **Hide –** The feature is **not** displayed during the installation process and when the user is adding or removing features in the Command AntiVirus installation program's **Add/Remove Application** dialog box. For more information, refer to **Installation Maintenance** in the ***Installation*** chapter of this administrator's guide.

  The feature is only hidden. It is installed and available to the user unless you set the installation state to **Entire feature will be unavailable**.

NOTE: If you hide a feature, then all of the subfeatures are also hidden.

- **Unhide** – The feature is displayed during the installation process and when the user is adding or removing features after CSAV is installed. This is the default.

14. Click **Next.** The system displays the **Identify Additional Servers** dialog box:



Identify Additional Servers

Specify additional network servers on which you have replicated the administrative installation point. Users can install from any of these servers.

Paths to replicated images of administrative installation points:

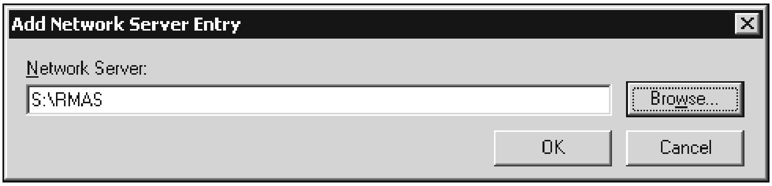
Identify Additional Servers Dialog Box

This dialog box allows you to specify additional network servers that have a copy of the installation folder tree. If you install features to run from the server or to be installed when the feature is first accessed, this option ensures that there is always access to an available network server.

Initially, the primary server is the server from which you installed Command AntiVirus. If this server is unavailable, an attempt is made to connect to each server in the list from top to bottom until a successful connection is made. If a connection is successful, the server that is connected now becomes the primary server.

If no server is available, the system prompts the user for the location of a server.

15. To add an additional network server, click **Add**. The system displays the **Add Network Server Entry** dialog box:



Add Network Server Entry

Network Server: S:\RMAS

Add Network Server Entry Dialog Box

16. In the **Network Server** text box, type the path and name of the server that you want to add, for example:

```
S:\RMAS
```

The drive letter <u>**must**</u> be mapped on the user’s computer. You can also specify a Universal Naming Convention (UNC) path.

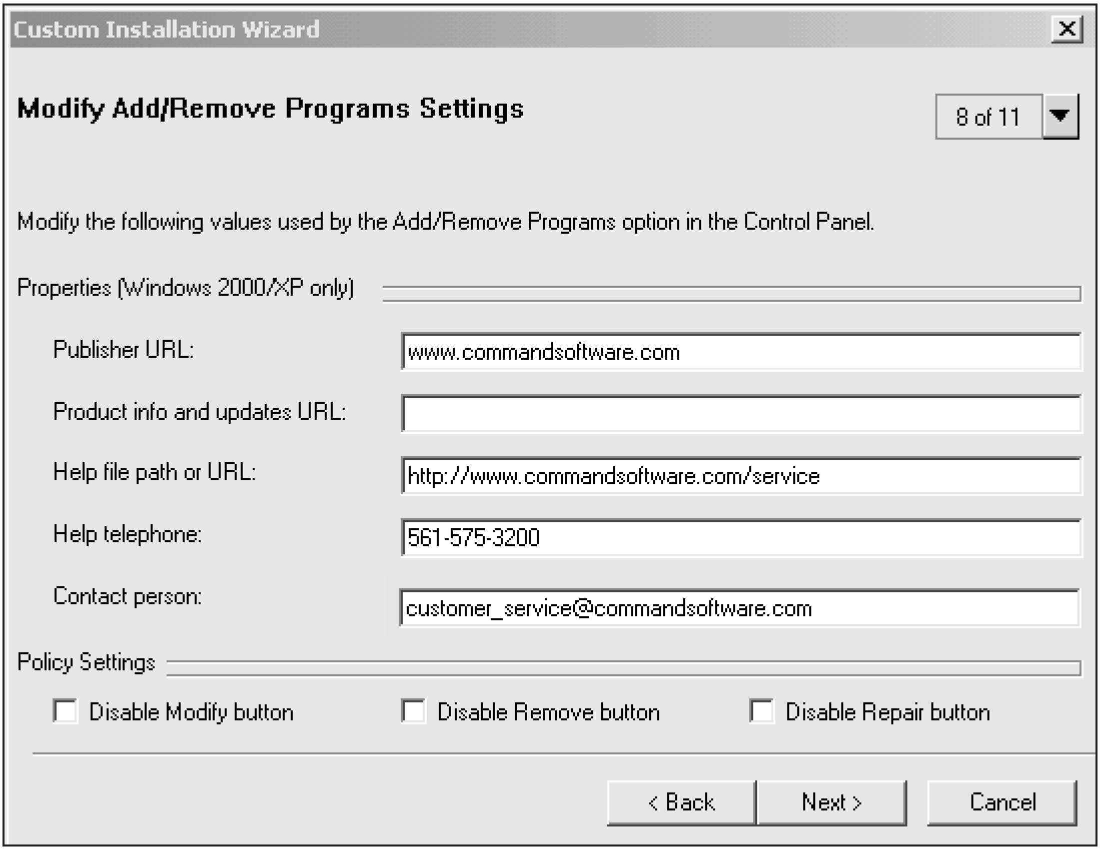
NOTE: Make sure that you type in a <u>**valid**</u> path and name. You can use the **Browse** button to search for the server.

17. Click **OK**. The system returns to the **Identify Additional Servers** dialog box. The **Server Folder Path** list box now contains the server that you added.

    Repeat **Steps 14** through **16** for each additional server that you want to add.

NOTE: To change a server, select a server in the list and click **Modify.** To delete a server, select a server in the list and click **Remove.** To change the position of a server in the list, select the server and click the up or down **Move** buttons.

18. Click **Next**. The system displays the **Modify Add/Remove Programs Settings** dialog box:



Custom Installation Wizard

Modify Add/Remove Programs Settings

Modify the following values used by the Add/Remove Programs option in the Control Panel.

Properties (Windows 2000/XP only)

Publisher URL: www.commandsoftware.com

Product info and updates URL:

Help file path or URL: http://www.commandsoftware.com/service

Help telephone: 561-575-3200

Contact person: customer_service@commandsoftware.com

Policy Settings

□ Disable Modify button □ Disable Remove button □ Disable Repair button

Modify Add/Remove Programs Settings Dialog Box

This dialog box allows you to modify the information that is displayed in the Windows **Support Info** dialog box for Command AntiVirus. You can access this information through the Windows **Add/Remove Programs** dialog box in the Control Panel. Select Command AntiVirus and click **support information**.

You can also disable the **Change** and **Remove** buttons for Command AntiVirus that are displayed in the Windows **Add/Remove Programs** dialog box and the **Repair** button that is displayed in the Windows **Support Info** dialog box for Command AntiVirus.

19. To change the default contact information, type the new information in the appropriate text boxes.

20. To disable the following buttons, select or clear the appropriate check boxes under **Policy Settings**. These check boxes are **not** selected by default.

    - **Disable Modify button** – Allows you to prevent the users from modifying Command AntiVirus. When this function is disabled, the **Change** button for Command AntiVirus that is displayed in the Windows **Add/Remove Programs** dialog box is dimmed.

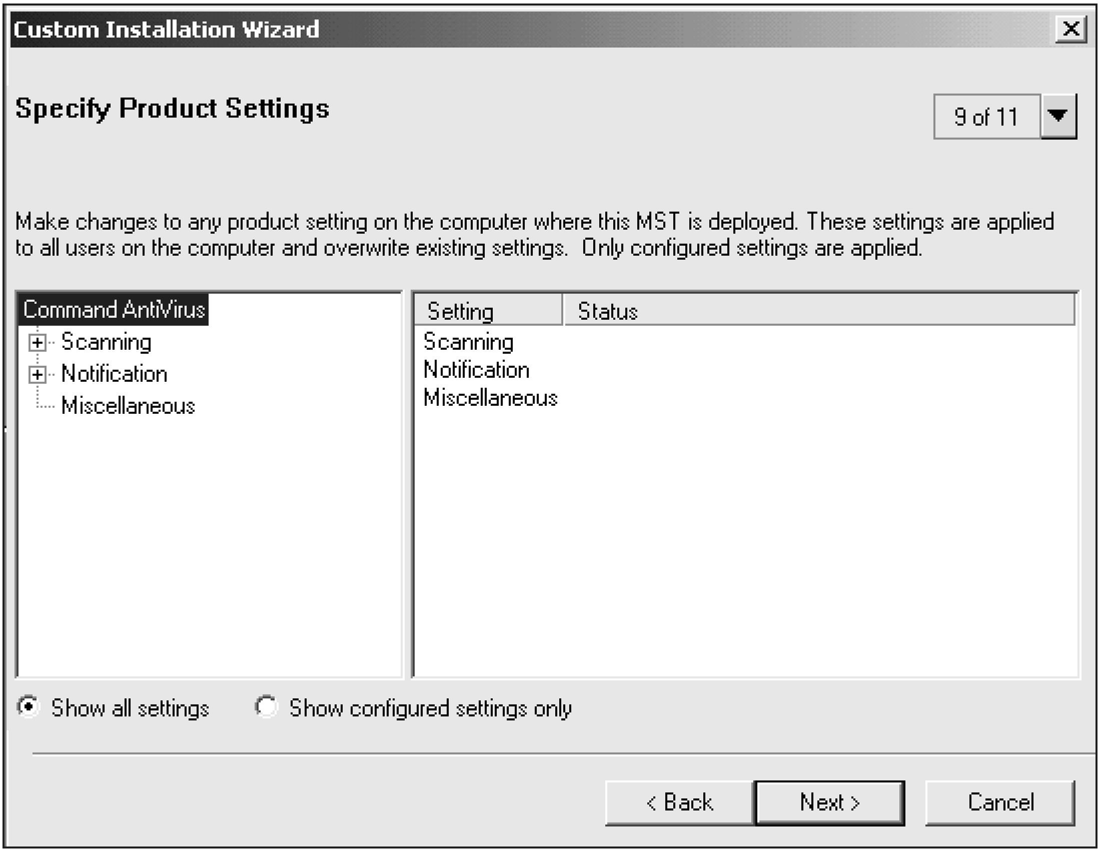
      For more information on making changes to Command AntiVirus after installation, refer to **Installation Maintenance** in the ***Installation*** chapter of this administrator's guide.

    - **Disable Remove button** – Allows you to prevent the users from removing Command AntiVirus through the Windows **Add/Remove Programs** dialog box. When this function is disabled, the **Remove** button for Command AntiVirus that is displayed in the Windows **Add/Remove Programs** dialog box is dimmed.

      For more information on removing Command AntiVirus through the Command AntiVirus installation program's **Add/Remove Application** dialog box, refer to **Installation Maintenance** in the ***Installation*** chapter of this administrator's guide.

    - **Disable Repair button** – Allows you to prevent the users from reinstalling Command AntiVirus through the Windows **Support Info** dialog box for Command AntiVirus. When this function is disabled, the **Repair** button is dimmed.

21. Click **Next**. The system displays the **Specify Product Settings** dialog box:



Custom Installation Wizard

Specify Product Settings

9 of 11

Make changes to any product setting on the computer where this MST is deployed. These settings are applied to all users on the computer and overwrite existing settings. Only configured settings are applied.

- Command AntiVirus
  - Scanning
  - Notification
  - Miscellaneous

Setting	Status
Scanning	
Notification	
Miscellaneous	

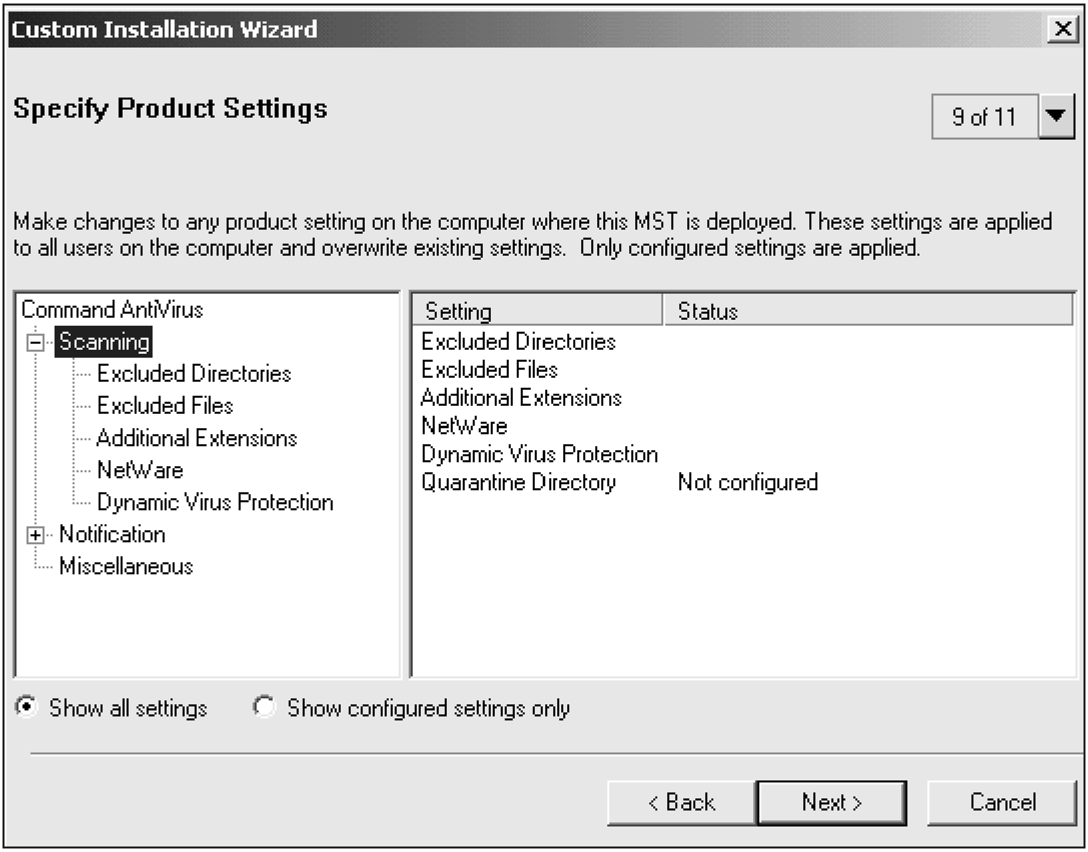
● Show all settings ○ Show configured settings only

Specify Product Settings Dialog Box

This dialog box allows you to modify the default installation settings for the items on the Command AntiVirus **Preferences** menu. For more information, refer to **Using the Preferences Menu** in the ***Using Command AntiVirus*** chapter of this administrator’s guide.

NOTE: If you have already configured these settings in the System Policy Template for Command AntiVirus and are going to use this **.ADM** file to set System Policy for this installation, you do not need to configure the settings here.

22. Click the plus sign (+) to the left of a **Preference** folder, for example, **Scanning**, to expand the folder:



Make changes to any product setting on the computer where this MST is deployed. These settings are applied to all users on the computer and overwrite existing settings. Only configured settings are applied.

Setting	Status
Excluded Directories	
Excluded Files	
Additional Extensions	
NetWare	
Dynamic Virus Protection	
Quarantine Directory	Not configured

● Show all settings ○ Show configured settings only

Specify Product Settings Dialog Box – Scanning Expanded

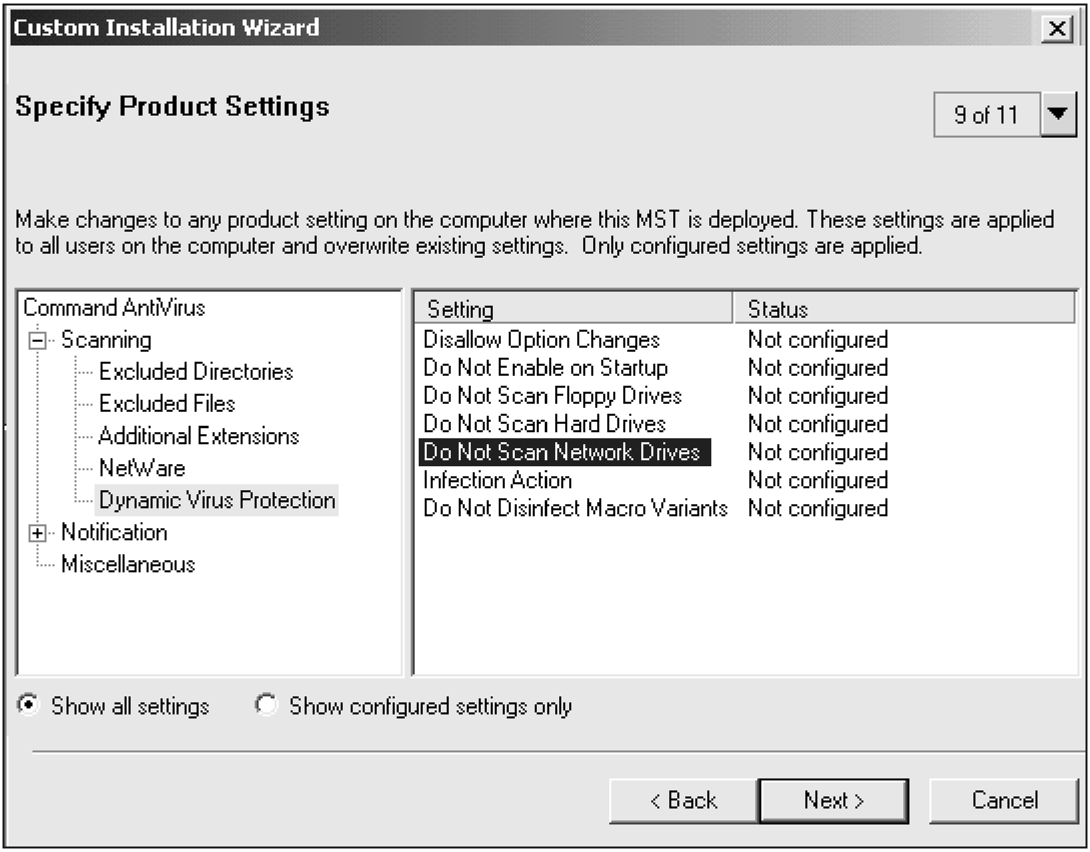
The **Specify Product Settings** window has two panes. The left-hand pane contains a list of the Command AntiVirus **Preferences** that you can configure.

When you select a **Preference**, by default, the right-hand pane contains a list of **Settings** for this **Preference**. The right-hand pane also shows the present **Status** of each setting, for example, **Configured** or **Not configured**.

Below the **Set Product Settings** window, there are two radio buttons that determine the list of **Settings** that you see in the right-hand pane. They are:

- **Show all settings** – lists all of the settings that you can configure.
- **Show configured settings only** – lists only the settings that you have configured.

23. In the left-hand pane, select a **Preference**, for example, **Dynamic Virus Protection**. The settings for **Dynamic Virus Protection** are displayed in the right-hand pane. The right-hand pane also shows the present **Status**, for example, **Not configured**:



Specify Product Settings

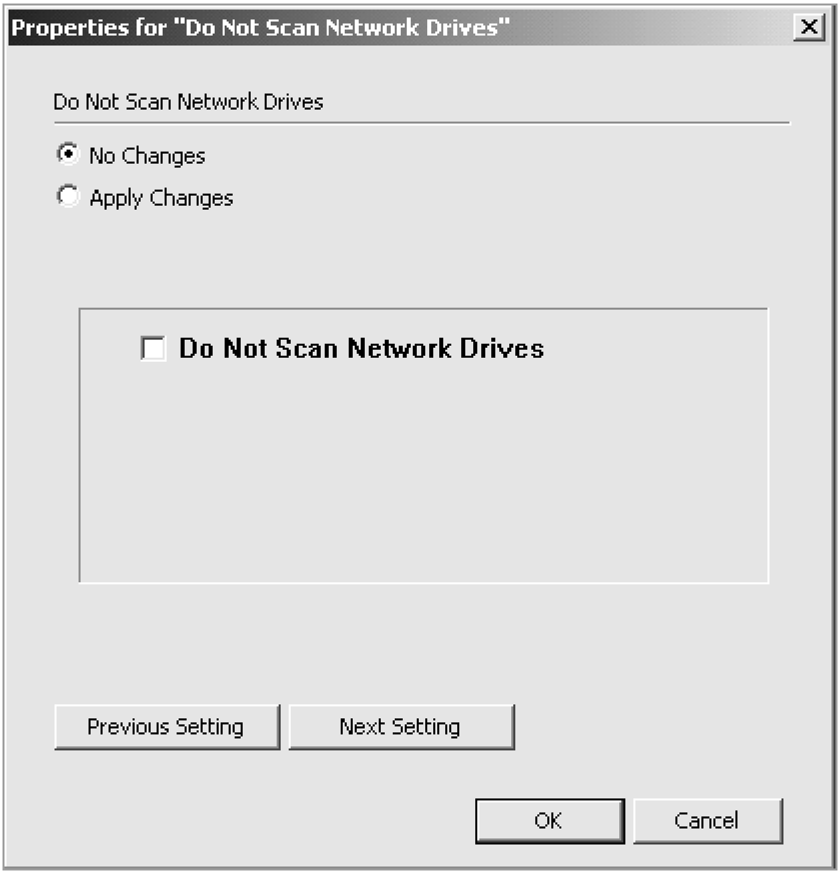
Make changes to any product setting on the computer where this MST is deployed. These settings are applied to all users on the computer and overwrite existing settings. Only configured settings are applied.

Setting	Status
Disallow Option Changes	Not configured
Do Not Enable on Startup	Not configured
Do Not Scan Floppy Drives	Not configured
Do Not Scan Hard Drives	Not configured
Do Not Scan Network Drives	Not configured
Infection Action	Not configured
Do Not Disinfect Macro Variants	Not configured

● Show all settings ○ Show configured settings only

Specify Product Settings – DVP – Do Not Scan Network Drives – Not Configured

24. Double-click a setting, for example, **Do Not Scan Network Drives**, to configure it. The system displays the **Properties for “Do Not Scan Network Drives”** dialog box:



Properties for "Do Not Scan Network Drives"

Do Not Scan Network Drives

● No Changes

○ Apply Changes

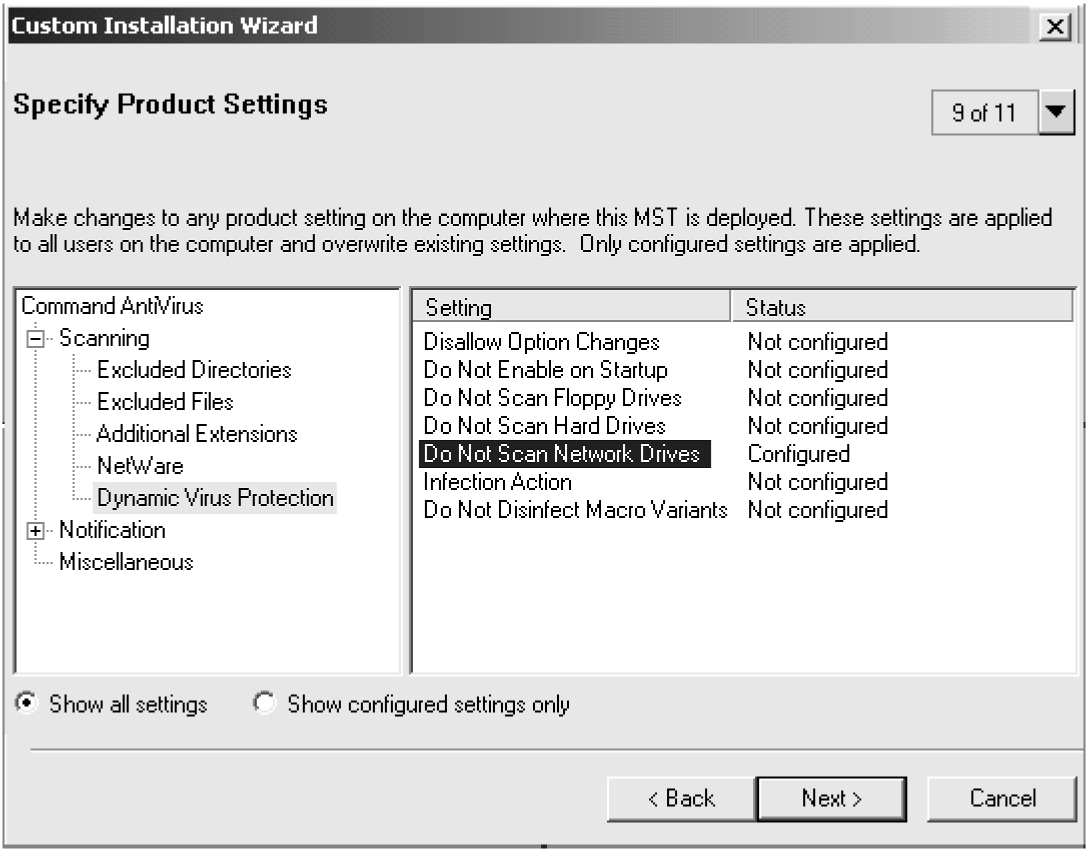
□ Do Not Scan Network Drives

Properties for “Do Not Scan Network Drives” Dialog Box

25. Select **Apply Changes**.

26. Select the settings that you want, for example, **Do Not Scan Network Drives**, and click **OK**. The system returns to the **Specify Product Settings** dialog box, and the **Do Not Scan Network Drives** settings now shows **Configured**.

NOTE: You can also use the **Previous Setting** and **Next Setting** buttons to configure other settings. The setting that you have just configured is saved by default.



Custom Installation Wizard

Specify Product Settings

Make changes to any product setting on the computer where this MST is deployed. These settings are applied to all users on the computer and overwrite existing settings. Only configured settings are applied.

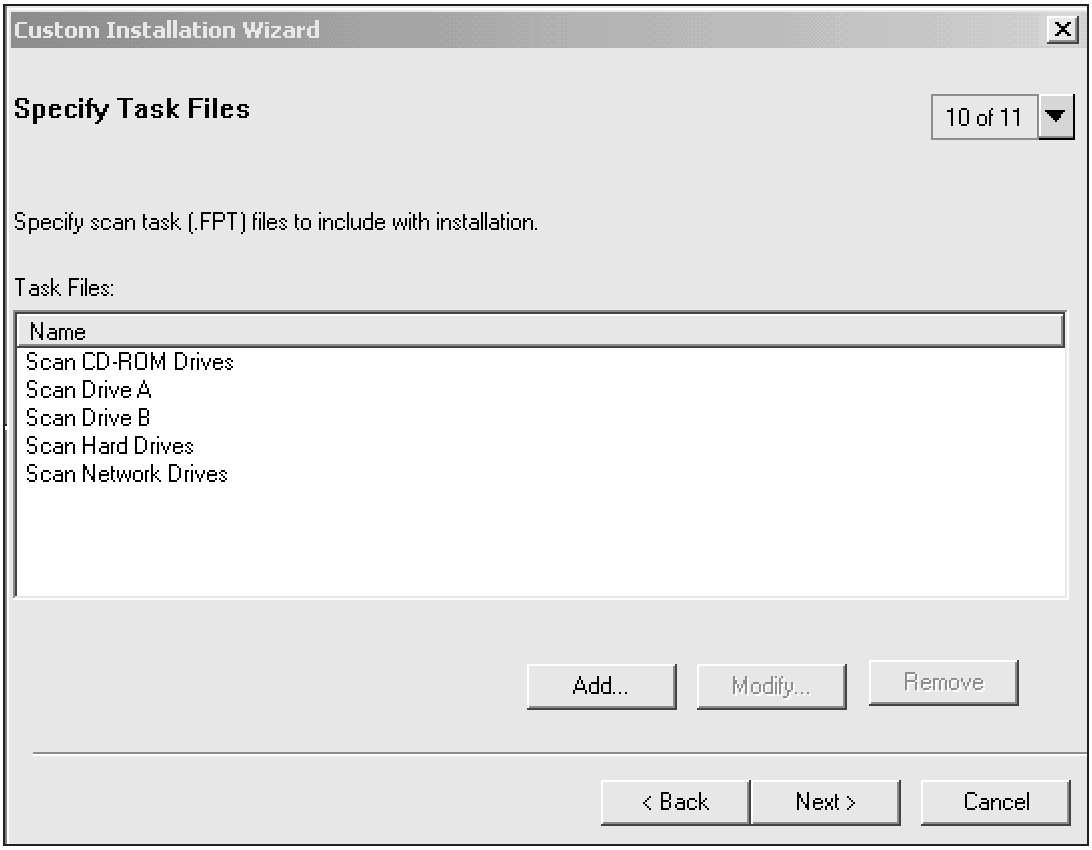
Setting	Status
Disallow Option Changes	Not configured
Do Not Enable on Startup	Not configured
Do Not Scan Floppy Drives	Not configured
Do Not Scan Hard Drives	Not configured
Do Not Scan Network Drives	Configured
Infection Action	Not configured
Do Not Disinfect Macro Variants	Not configured

● Show all settings ○ Show configured settings only

Specify Product Settings – DVP – Do Not Scan Network Drives – Configured

27. Repeat Steps 23 through 25 for each **Preference** and setting that you want to customize.

28. Click **Next**. The system displays the **Specify Task Files** dialog box:



Custom Installation Wizard

Specify Task Files

Specify scan task (.FPT) files to include with installation.

Task Files:

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

Specify Task Files Dialog Box

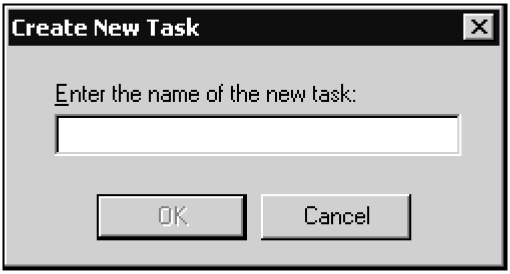
This dialog box allows you to customize the scan tasks that are available upon installation by:

- Creating new scan tasks.
- Modifying the **Properties** of the preconfigured **System Tasks** that come with Command AntiVirus.
- Removing the preconfigured **System Tasks** that come with Command AntiVirus.

29. Use the **Add**, **Modify**, or **Remove** buttons to customize the scan tasks.

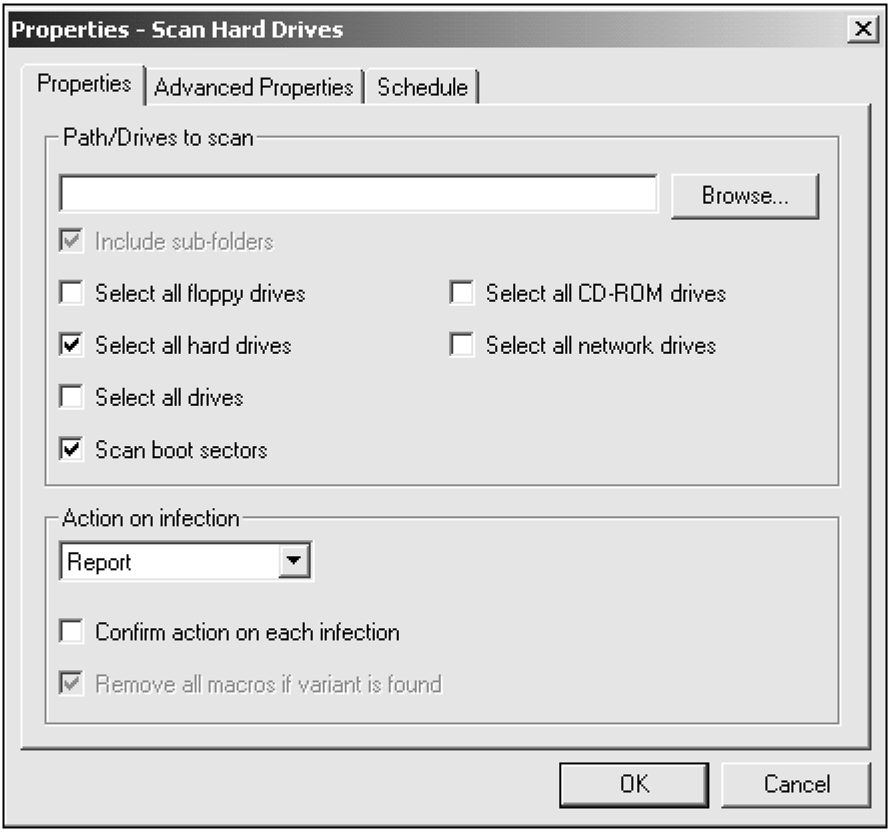
To create a new scan task, follow these steps:

A. Click the **Add** button. The system displays the **Create New Task** dialog box:



Create New Task Dialog Box

B. In the **Enter the name of the new task** text box, type the name of the new task, and click **OK**. The system displays the **Properties** dialog box:



Properties - Scan Hard Drives

Path/Drives to scan

☑ Include sub-folders

□ Select all floppy drives

□ Select all CD-ROM drives

☑ Select all hard drives

□ Select all network drives

□ Select all drives

☑ Scan boot sectors

Action on infection

Report

□ Confirm action on each infection

☑ Remove all macros if variant is found

Properties Dialog Box

C. Accept the default settings, or customize the settings to your needs, and click **OK**.

For more information, refer to **Configuring Scanning Properties** in the ***Using Command AntiVirus*** chapter of this administrator's guide.

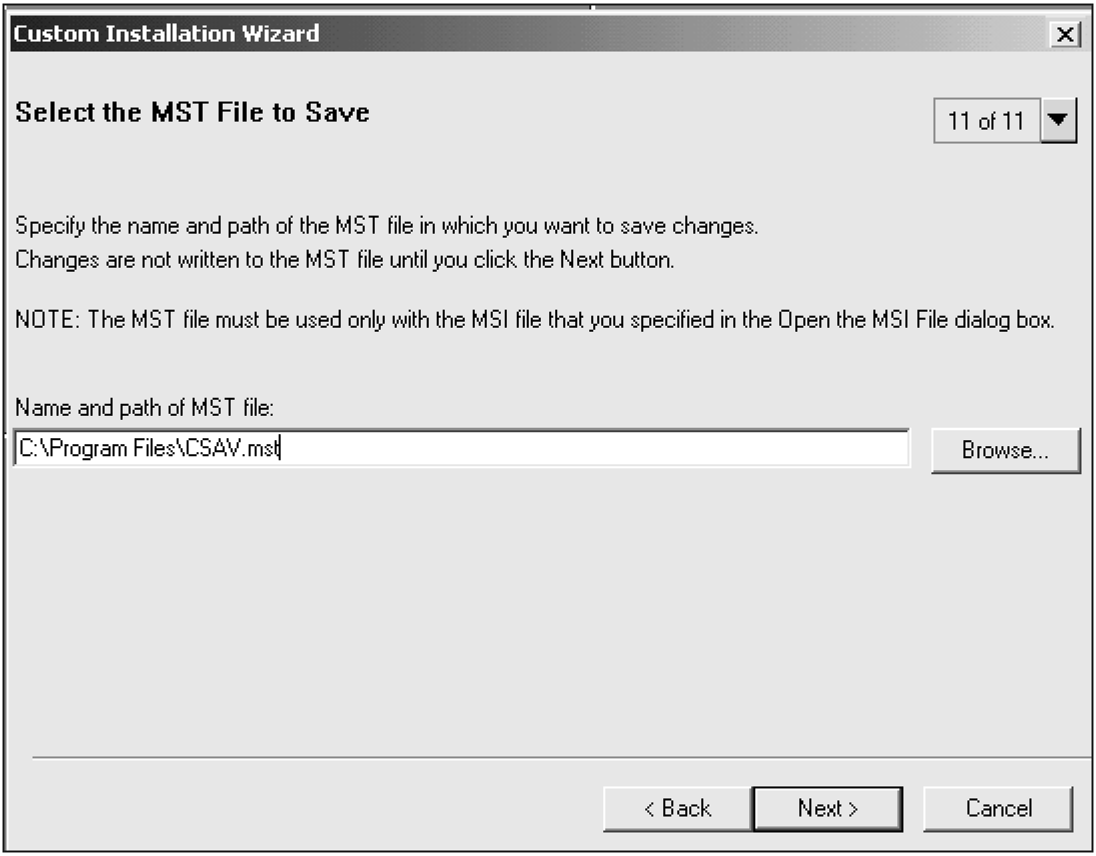
To modify an existing scan task, follow these steps:

A. Select a scan task, and click the **Modify** button. The system displays the **Properties** dialog box.

B. Accept the default settings, or customize the settings to your needs, and click **OK**.

To remove an existing scan task, select a scan task, and click the **Remove** button.

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



Select the MST File to Save

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

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

Name and path of MST file:
C:\Program Files\CSAV.mst

Select the MST File to Save Dialog Box

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

NOTE: If you are using the Custom Installation Wizard within the Command AntiVirus Deployment Prep Wizard, the path is set by default, and the text box is unavailable

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

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

The changes are not written to the MST file until you click Next.

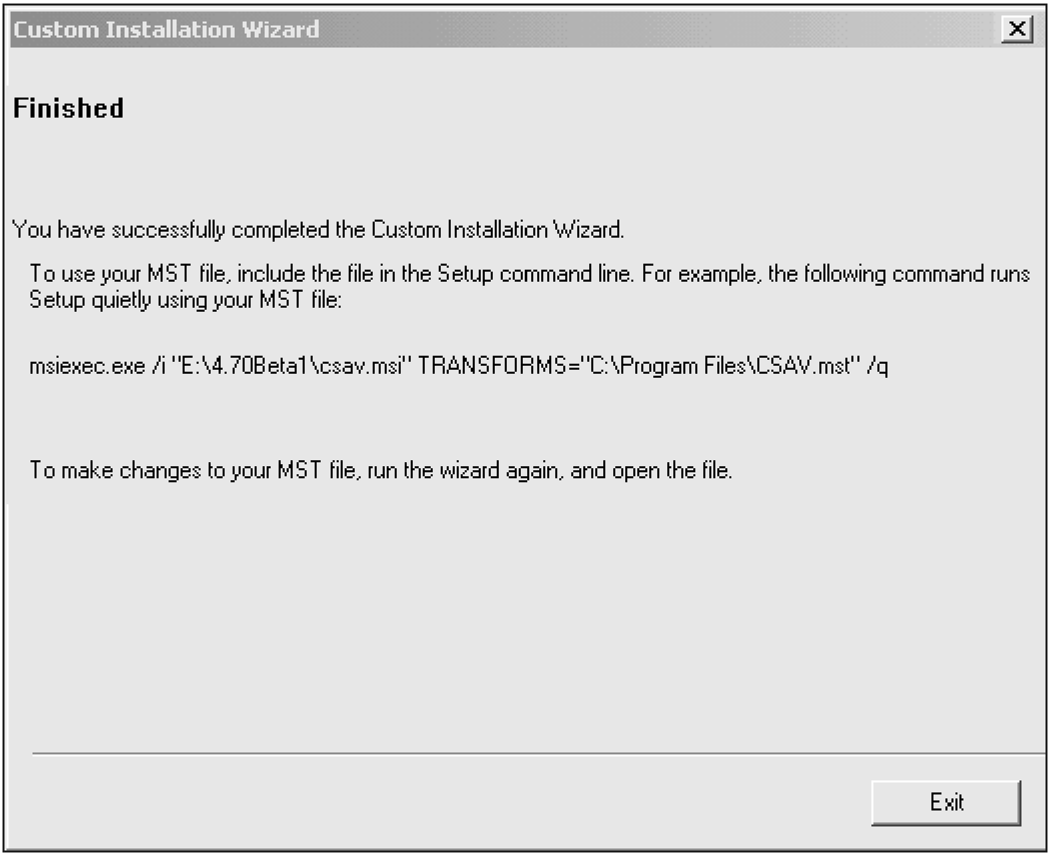
NOTE: You can also use the **Browse** button to search for a file and/or path.

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

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

32. Click **Next** to save your changes to the specified file. The system displays the **Finished** dialog box.

NOTE: If you need to modify your choices, click **Back**.



Custom Installation Wizard

Finished

You have successfully completed the Custom Installation Wizard.

To use your MST file, include the file in the Setup command line. For example, the following command runs Setup quietly using your MST file:

```
msiexec.exe /i "E:\4.70Beta1\csav.msi" TRANSFORMS="C:\Program Files\CSAV.mst" /q
```

To make changes to your MST file, run the wizard again, and open the file.

Finished Dialog Box

33. Click **Exit** to end the program.

If you want to make changes to an MST file, run the Command AntiVirus Custom Installation Wizard again, and open the MST file.

NOTE: For information on deploying your customized installation of Command AntiVirus to multiple users over the network, refer to **Starting the Installation Process** located in the ***Network Administration*** chapter of this administrator’s guide.

COMMAND ANTIVIRUS DOWNLOAD MANAGER

The Command AntiVirus Download Manager allows you to schedule automatic downloads of Command AntiVirus virus definition file (deffile) updates, component updates, and full product upgrades.

You can also configure the Command AntiVirus Download Manager to automatically apply the deffile and component updates to administrative images. Command AntiVirus for Windows contains an agent that detects a change in the administrative image and updates automatically the next time the user logs on to the machine. For more information, refer to **Updating Command AntiVirus** located in the ***Network Administration*** chapter of this administrator’s guide.

The Download Manager also allows you to create an administrative image of a downloaded upgrade of Command AntiVirus. You can create this image on a single server or on multiple servers by creating a directory share. From these multiple Software Distribution Points (SPDs), you can then advertise Command AntiVirus.

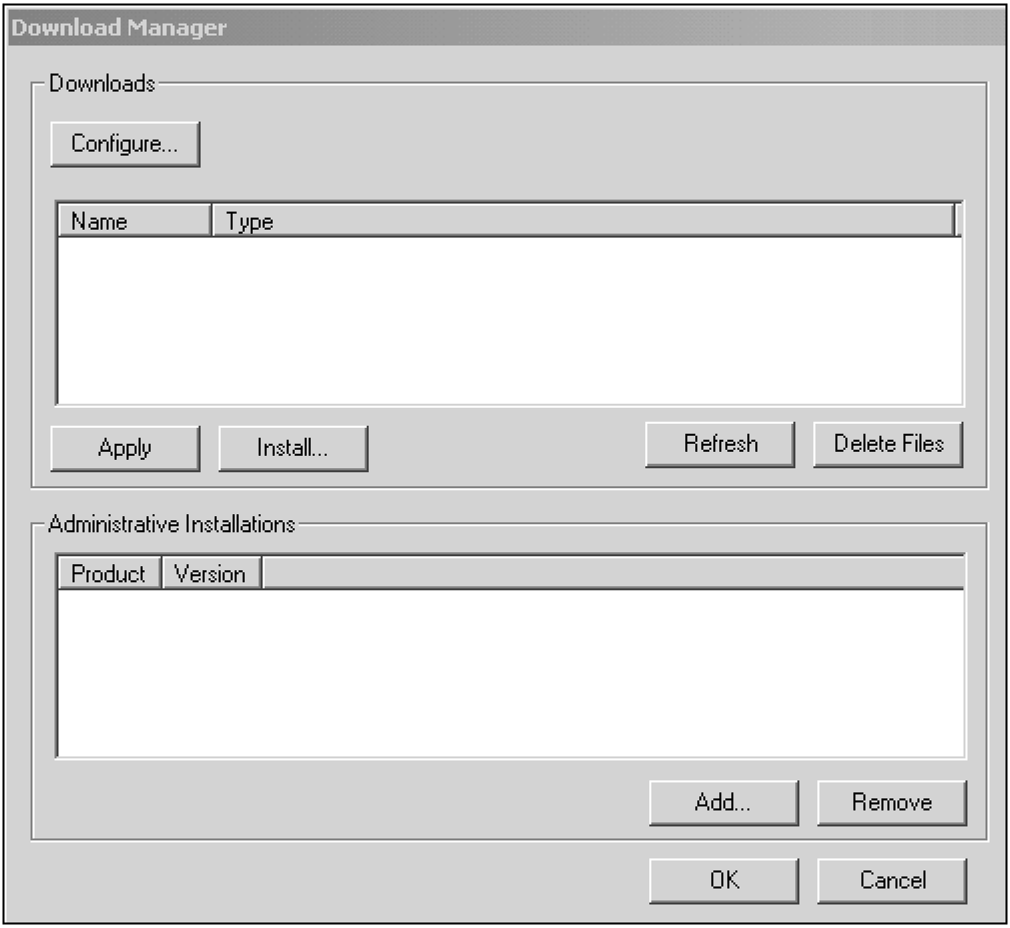
For more information on installing Command AntiVirus to a Software Distribution Point, refer to **Installing Command AntiVirus To A Software Distribution Point (SDP)** located in the ***Network Administration*** chapter of this administrator’s guide.

From the **Download Manager Main** dialog box, you can:

- Configure the download process
- Apply downloaded updates to administrative images
- Create an administrative image from a downloaded upgrade of Command AntiVirus
- Refresh the **Downloads** window
- Delete downloaded files
- Add administrative images to the **Administrative Installations** window
- Remove administrative images from the **Administrative Installations** window

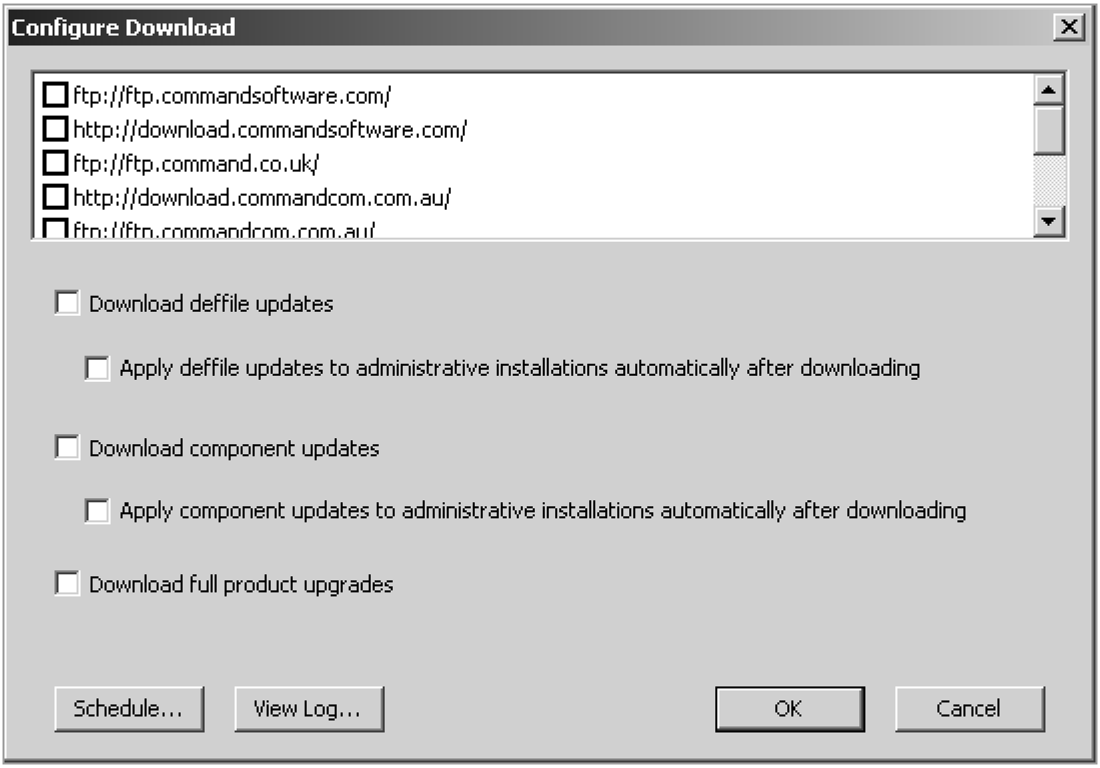
To start the Command AntiVirus Download Manager and configure the download process, follow these steps:

1. Click the **Start** button on the Windows taskbar.
2. Select **Programs**.
3. Select **COMMANDCentral**.
4. Click **CSAV Download Manager**. The system displays the **Download Manager Main** dialog box:



Download Manager Main Dialog Box

5. Click **Configure**. The system displays the **Configure Download** dialog box:



Configure Download

- □ ftp://ftp.commandsoftware.com/
- □ http://download.commandsoftware.com/
- □ ftp://ftp.command.co.uk/
- □ http://download.commandcom.com.au/
- □ ftp://ftp.commandcom.com.au/

□ Download deffile updates

□ Apply deffile updates to administrative installations automatically after downloading

□ Download component updates

□ Apply component updates to administrative installations automatically after downloading

□ Download full product upgrades

Configure Download Manager Dialog Box

6. Under **Sites**, select the check boxes of the download sites that your are authorized for or have purchased from:
   - **Command Software US** – Select the Command Software web site and FTP site. These are the first and second check boxes.
   - **Command Software UK** – Select the Command Software UK FTP site and web site. These are the third and fourth check boxes.
   - **Command Software Australia** – Select the Command Software Australia web site. This is the fifth check box.

When you select a check box, the system displays a **User Name and Password** dialog box. Enter a valid user name and password for the selected site, and click **OK.**

NOTE: After you enter a **valid** user name and password for a specific **Site**, this dialog box does **not** display again as long as the check box remains selected.

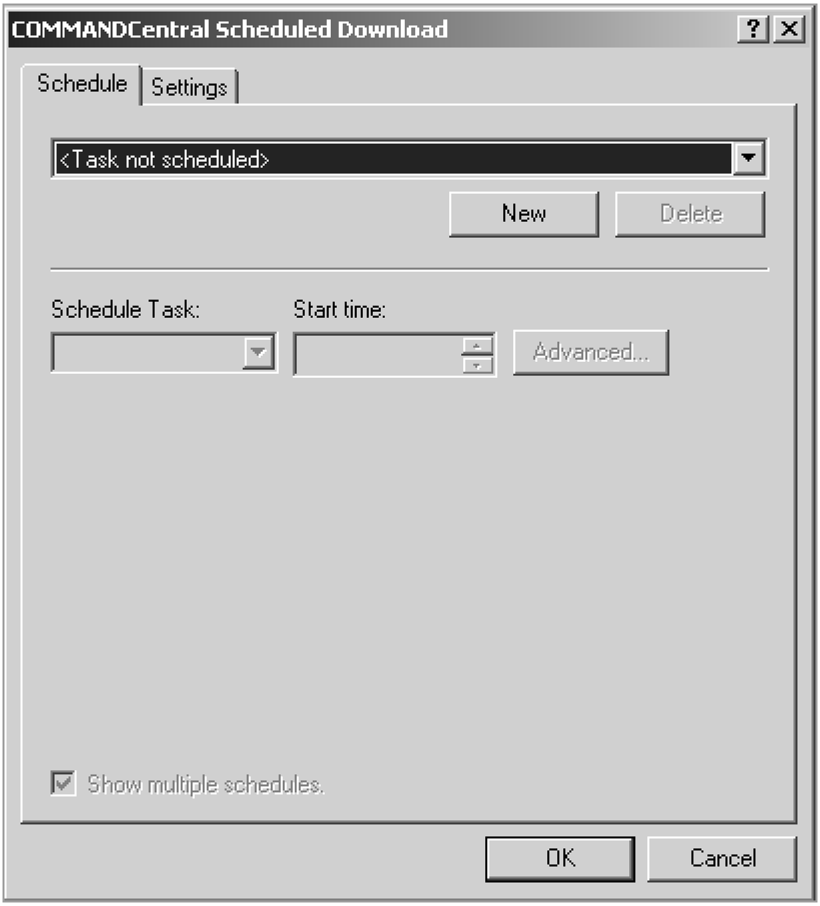
When a scheduled download takes place, the selected site at the top of the list is tried first. The selected site at the bottom is tried last.

7. Specify the type of updates and/or upgrades that you want to download. For the deffile and component updates, also specify if you want to apply the updates to administrative installations automatically after downloading the files.

   Select one or more of the following check boxes:

   - **Download deffile updates** – downloads the latest virus definition files if they have changed since the last download.
     - **Apply deffile updates to administrative installations automatically after downloading** – automatically applies the virus definition updates to administrative images after downloading.
   - **Download component updates** – downloads the latest component updates if there are any since the last download.
     - **Apply component updates to administrative installations automatically after downloading** – automatically applies the component updates to administrative images after downloading.
   - **Download full product upgrades** – downloads the latest version of Command AntiVirus if there are any since the last download.

8. Click the **Schedule** button. The system displays the **COMMANDCentral Scheduled Download** dialog box:



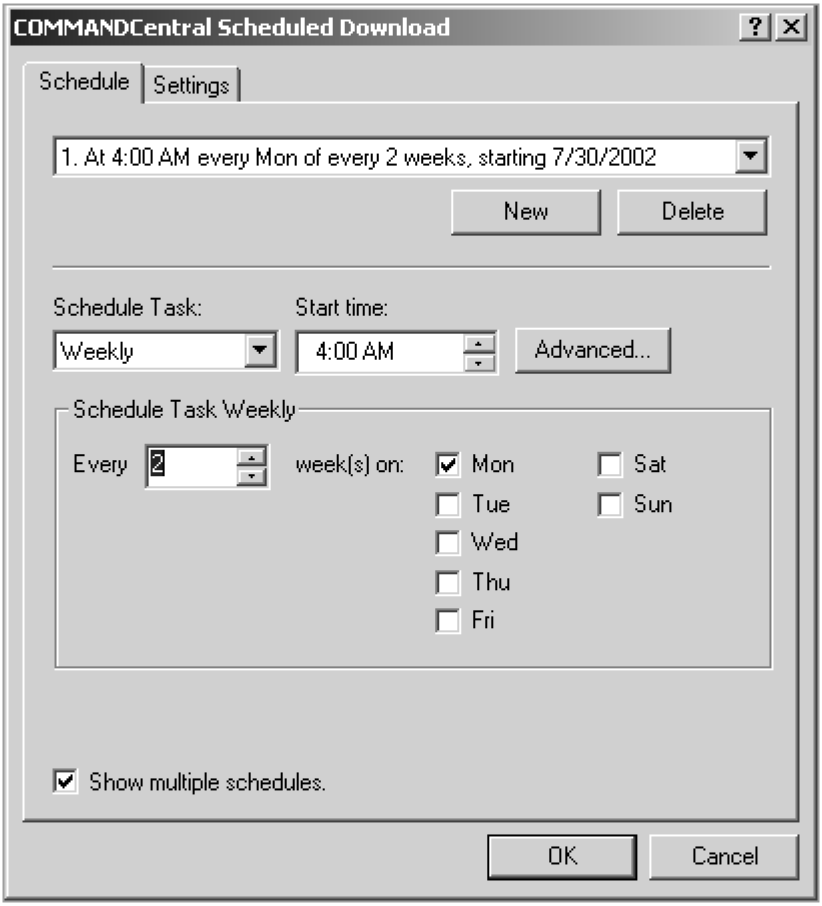
COMMANDCentral Scheduled Download Dialog Box

9. In the **Schedule** dialog box, click the **New** button to create a new task.

10. In the **Schedule Task** list, click the drop-down arrow, and select how frequently you want the downloads to occur, for example, **Daily**, **Weekly**, **Monthly**, etc.

11. Depending on the selection that you made in **Step 11**, make the appropriate selections under **Schedule Task XXX**.

    For example, if you selected **Weekly**, under **Schedule Task Weekly**, select how often and the day of the week that you want the downloads to occur. If you want the download to occur every 2 weeks on a Monday, in the **Every** box select **2**, and then, select the **Mon** check box.



COMMANDCentral Scheduled Download

1. At 4:00 AM every Mon of every 2 weeks, starting 7/30/2002

Schedule Task: Weekly

Start time: 4:00 AM

Schedule Task Weekly

Every 2 week(s) on: ☑ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

☑ Show multiple schedules.

Schedule Dialog Box

12. In the **Start time** box, click the **up** or **down** arrows to select a time for the download to start, for example, 4 AM.

13. Click **OK** to save the schedule. The system returns to the **Configure Downloads** dialog box.

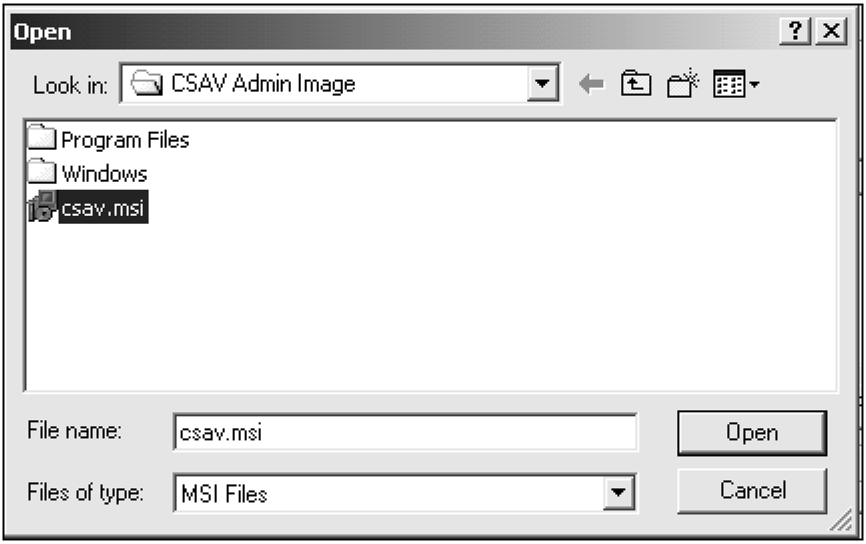
In Windows 2000, Windows XP, and Windows NT, the system first displays the **Set Account Information** dialog box. Enter a user name and password for an account that has Internet access to download the updates and the rights to apply the updates to administrative images.

NOTE: You can view the details of the download by clicking the **View Errors** button. The system displays an **Error Log**.

14. Click **OK**. The system returns to the **Download Manager Main** dialog box.

15. Under **Administrative Installations**, click the **Add** button. The system displays the **Open** dialog box.

16. Browse to a folder that contains a Command AntiVirus administrative image that you want to apply the updates to, for example, Command AntiVirus 4.70.0:



Open

Look in: CSAV Admin Image

Program Files

Windows

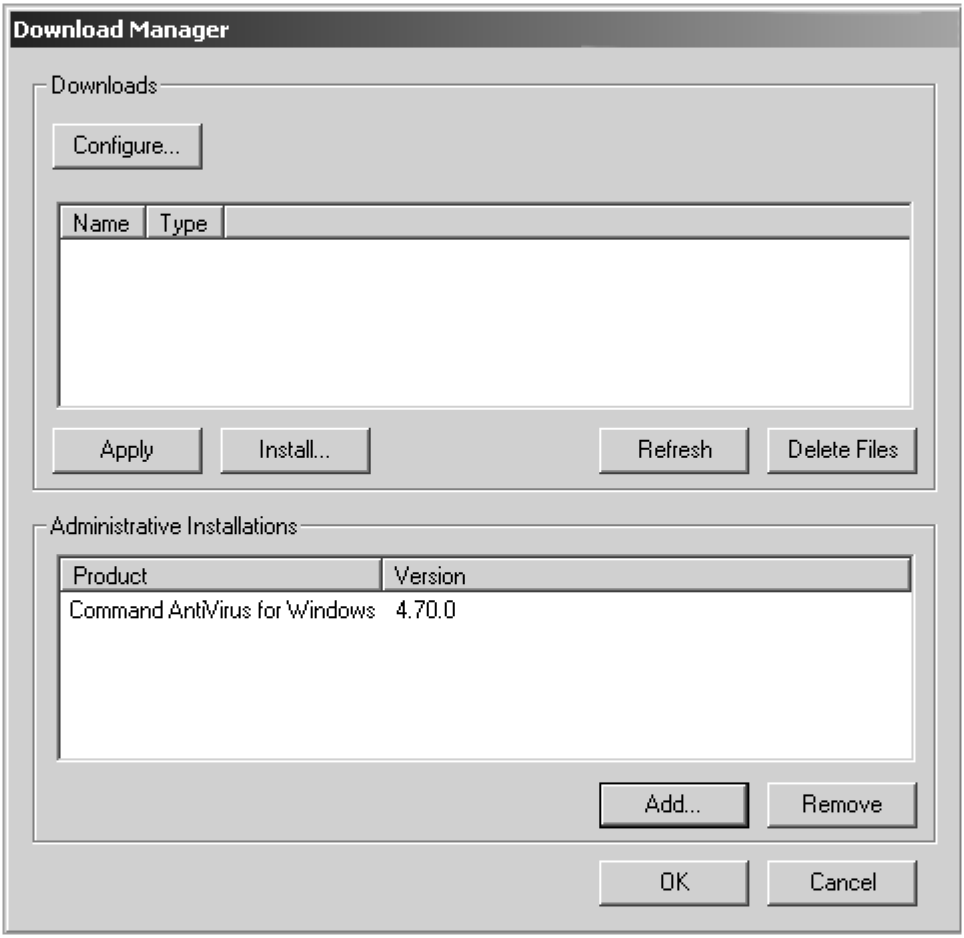
csav.msi

File name: csav.msi

Files of type: MSI Files

Open Dialog Box

17. Select the **MSI**, and click **Open**. The system returns to the **Download Manager Main** dialog box. Command AntiVirus for Windows 4.70.0 is now shown in the **Administrative Installations** window:

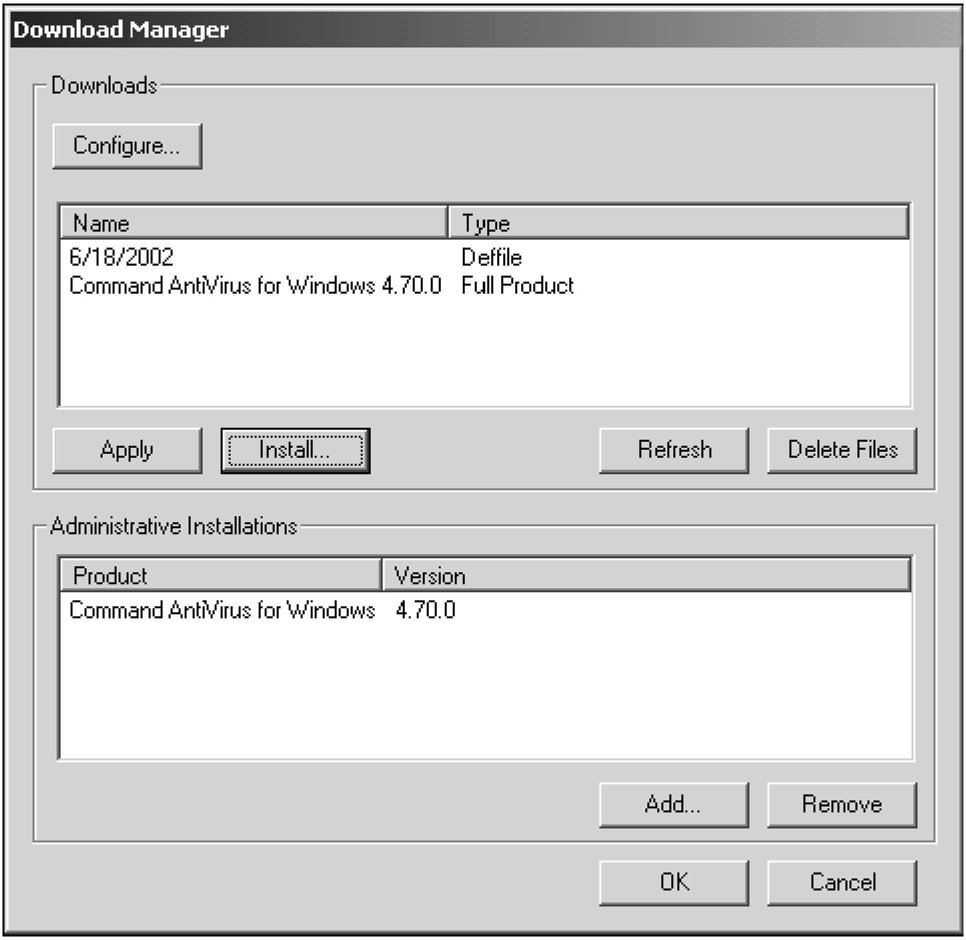


Product	Version
Command AntiVirus for Windows	4.70.0

Download Manager Main Dialog Box – Administrative Installations Window

18. Repeat **Steps 16** and **17** for any additional administrative images that you want to add.

When the updates and upgrades are downloaded, the files are listed in the **Downloads** window of the **Download Manager Main** dialog box:



Name	Type
6/18/2002	Deffile
Command AntiVirus for Windows 4.70.0	Full Product

Product	Version
Command AntiVirus for Windows	4.70.0

Download Manager Main Dialog Box – Downloads Window

If a download occurs while the **Download Manager Main** dialog box is open, the list is not updated until you click the **Refresh** button, or you close the **Download Manager Main** dialog box and reopen it.

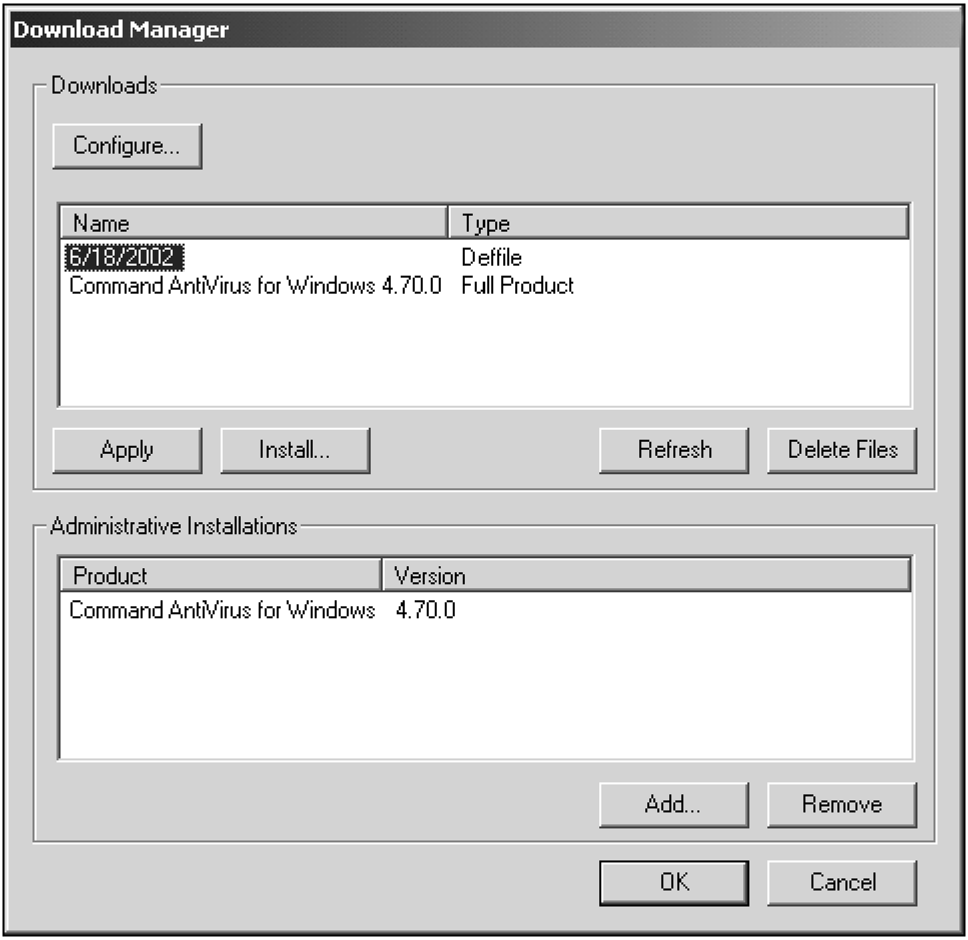
To delete download files, select the file, and click the **Delete Files** button. This action deletes the file from the **Downloads** window and deletes the file from the download folder.

NOTE: If you selected to apply deffile and component updates to administrative installations automatically after downloading, the updates are applied to the administrative images listed in the **Administrative Installations** window. The updates are installed automatically the next time the user logs on to the machine.

To remove an administrative image from the list, select the image, and click the **Remove** button. This action only removes the image from the list. It does **not** delete any files.

Applying the Downloaded Updates Manually

If you did not select to apply deffile and component updates to administrative installations automatically after downloading, you can apply them manually.



Name	Type
6/18/2002	Deffile
Command AntiVirus for Windows 4.70.0	Full Product

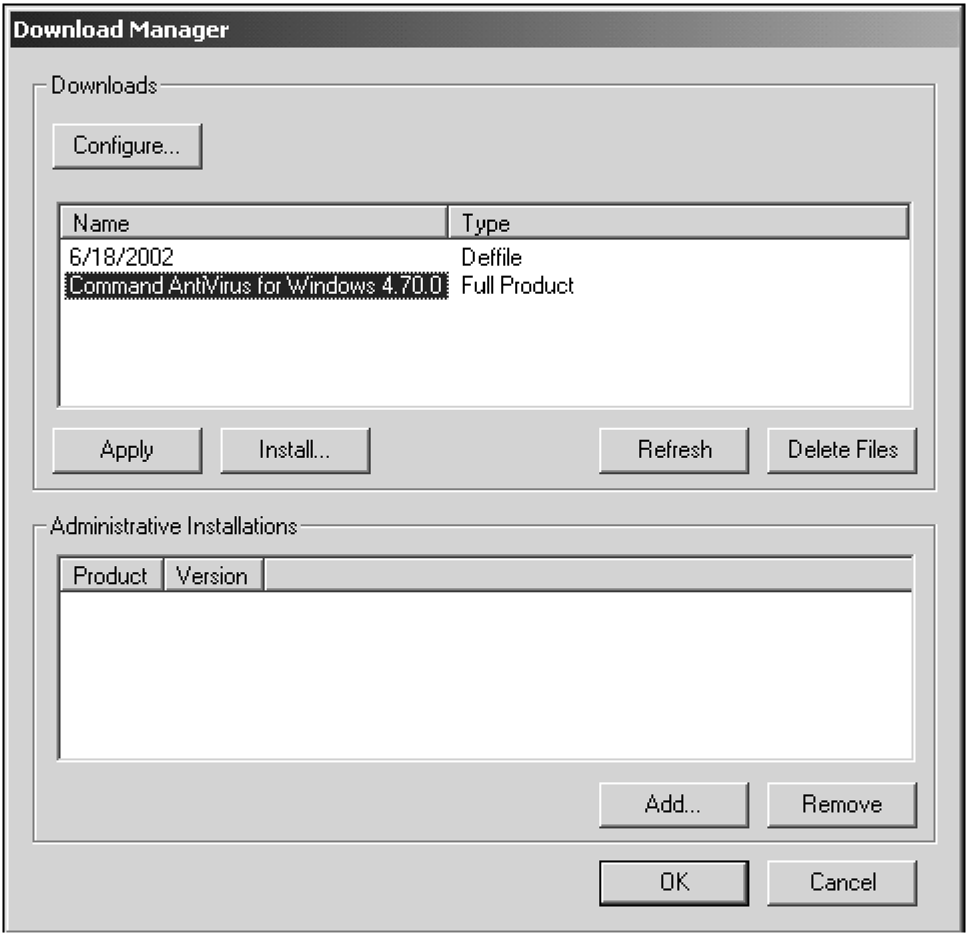
Product	Version
Command AntiVirus for Windows	4.70.0

Downloads Window – Apply Updates

To apply deffile and component updates to administrative installations manually, in the **Downloads** window, select an update, and click the **Apply** button. The update is applied to the administrative images listed in the **Administrative Installations** window. The updates are installed automatically the next time the user logs on to the machine.

Creating an Administrative Image of a Downloaded Upgrade

The Download Manager allows you to create an administrative image of a downloaded upgrade of Command AntiVirus. You can create this administrative image on a single server or in Windows NT and Windows 2000/XP on multiple servers by creating a directory share. From these multiple Software Distribution Points (SPDs), you can then advertise Command AntiVirus.

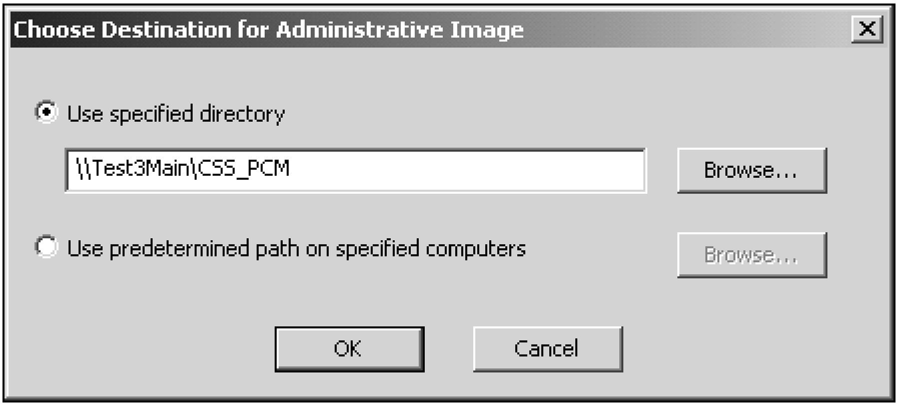


Name	Type
6/18/2002	Deffile
Command AntiVirus for Windows 4.70.0	Full Product

Downloads Window – Create Administrative Image

To create an administrative image of a downloaded full product upgrade, follow these steps:

1. In the **Downloads** window, select the upgrade, and click **Install.** The system displays the **Choose Destination for Administrative Image** dialog box:


Choose Destination for Administrative Image

● Use specified directory

\\Test3Main\CSS_PCM

○ Use predetermined path on specified computers

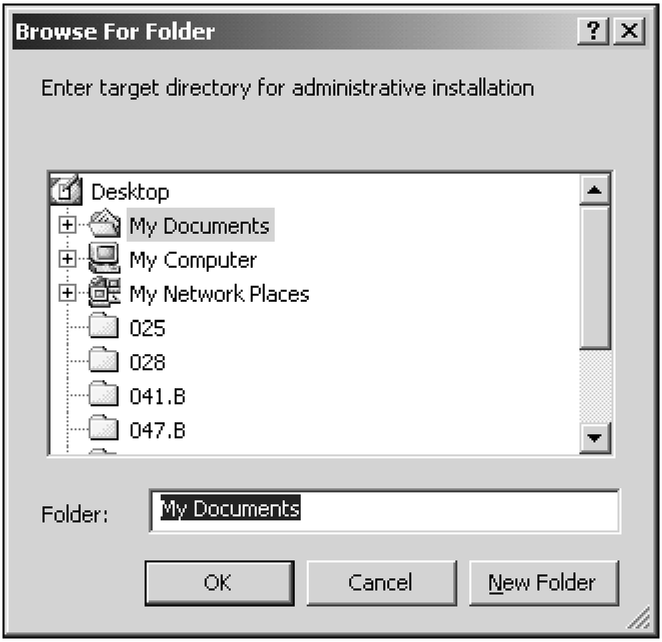
Choose Destination for Administrative Image

2. Select <u>**one**</u> of the following:

NOTE: If you are administering your network from a Windows 95/98/Me machine, you must select the **Use specified directory** option.

- **Use specified directory** – Allows you to create an administrative image on a single server. You can specify both the installation drive and path. The drive can be a local or network drive, and the path can be a normal or Universal Naming Convention (UNC) path.

  Click the **Browse** button. The system displays the **Browse For Folder** dialog box:



Enter target directory for administrative installation

Folder: My Documents

Browse For Folder

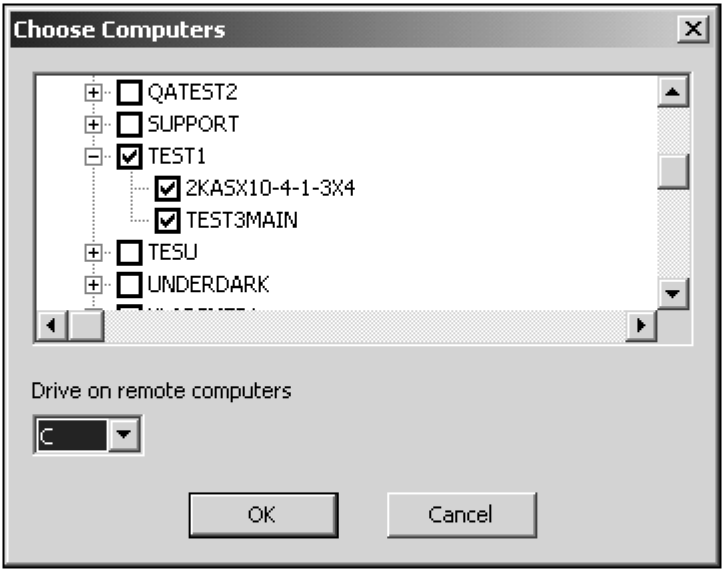
Select the installation drive and path, and click **OK**. The system returns to the **Choose Destination for Administrative Image** dialog box.

Continue with **Step 3**.

- **Use predetermined path on specified computers** – Allows you to create an administrative image on multiple servers by creating a directory share. You can specify **only** the computers that you want to select and the installation drive. A common predetermined path is created on the specified drive.

NOTE: The selected installation drive and the predetermined path are the same for **all** of the selected computers.

Click the **Browse** button. The system displays the **Choose Computers** dialog box:



Choose Computers

- ☐ QATEST2
- ☐ SUPPORT
- ☑ TEST1
  - ☑ 2KASX10-4-1-3X4
  - ☑ TEST3MAIN
- ☐ TESU
- ☐ UNDERDARK

Drive on remote computers: C

Choose Computers Dialog Box

In the **Choose Computers** list, select the machines on which you want to install the administrative image. Click the plus sign (**+**) to the left of a domain to expand it, for example, **TEST1**.

You can select an entire domain or individual machines by clicking the check box to the left of the domain or machine name. For example, to select **all** of the machines in the **TEST1** domain, click the check box to the left of **TEST1**.

In the **Drive on remote computers** text box, click the drop-down arrow to select the installation drive letter, and click **OK**. The system returns to the **Choose Destination for Administrative Image** dialog box

NOTE: The selected installation drive is the same for **all** of the selected computers.

Continue with **Step 3**.

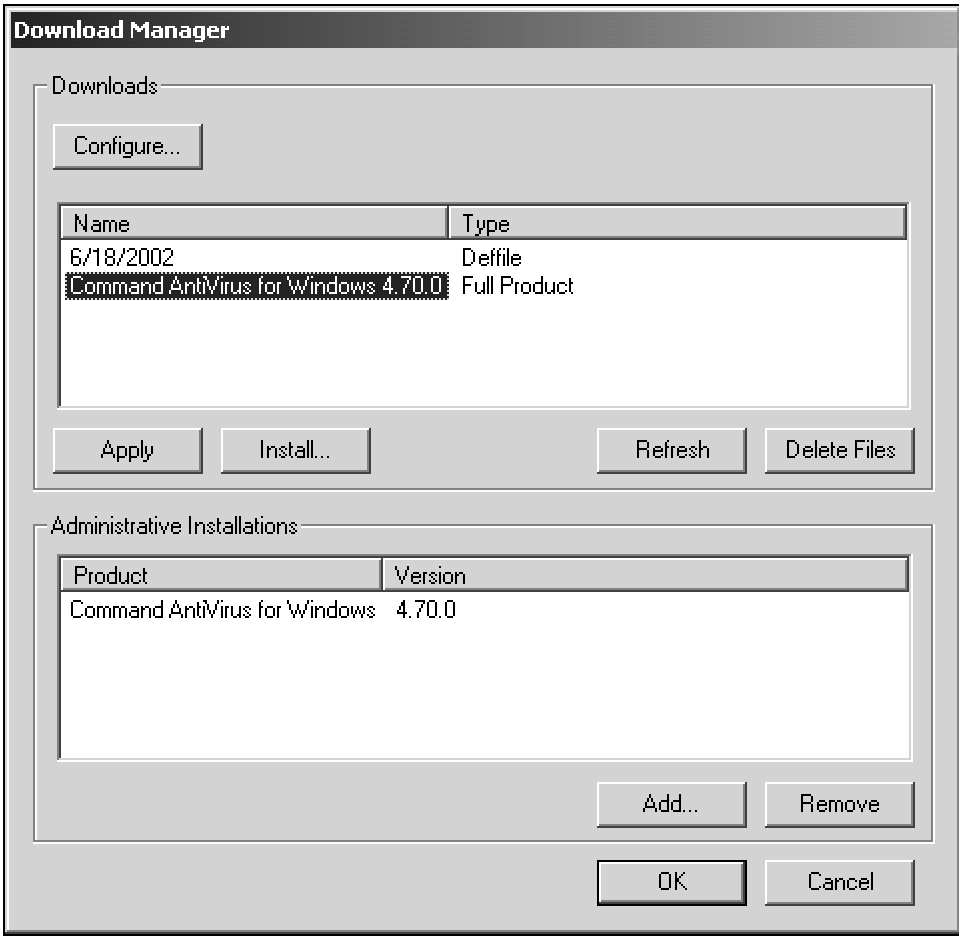
3. Click **OK**. The program begins creating the administrative image.

   The system displays the **Updating System** dialog box. Please wait while the program copies the files to the Software Distribution Point (SDP).

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

If you are creating multiple SPDs and the installation of the administrative image on one of the SPDs fails, the process ends. Software distribution points and administrative images created prior to the error are complete. All SPDs and administrative images yet to be created are **not** complete.

When the copying is complete, the system returns to the **Download Manager Main** dialog box:



Name	Type
6/18/2002	Deffile
Command AntiVirus for Windows 4.70.0	Full Product

Product	Version
Command AntiVirus for Windows	4.70.0

Downloads Window – Apply Updates

The administrative image is added to the list in the **Administrative Installations** window.

NOTE: We recommend that you copy the administrative image to another location in your network. This provides a backup copy when an installation needs to be repaired. This copy is **only** for backup purposes. Command AntiVirus can only be installed from the location from which it was advertised.

INSTALLATION MAINTENANCE

After you have installed COMMANDCentral, you can reinstall or remove COMMANDCentral through the installation program's **Application Maintenance** dialog box.

2K/XP

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

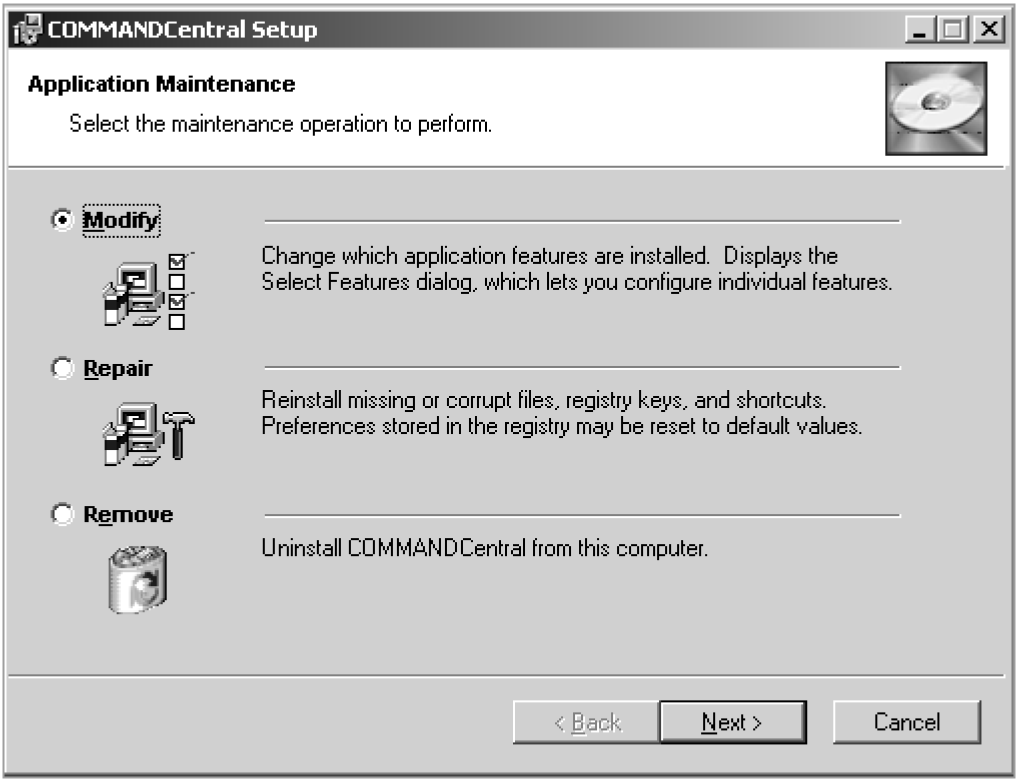
NT/2K/XP

In Windows NT, Windows 2000, or Windows XP, to perform any of the installation maintenance tasks, **one** of the following conditions **must** be met:

- You are a member of the Administrators group on the local machine
- System policy is set so that you have elevated privileges for installations

To start the installation program, follow these steps:

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



COMMANDCentral Setup

Application Maintenance

Select the maintenance operation to perform.

● **Modify**

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

○ **Repair**

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

○ **Remove**

Uninstall COMMANDCentral from this computer.

Application Maintenance Dialog Box

This dialog box contains the following operations:

- **Modify** – allows you to add or remove features or subfeatures.

NOTE: In COMMANDCentral there are no features to add or remove.

- **Repair** – allows you to reinstall missing or corrupt files, registry keys, and shortcuts.
- **Remove** – allows you to remove COMMANDCentral completely.

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

REINSTALLING COMMANDCENTRAL

You can repair the COMMANDCentral through the installation program's **Application Maintenance** dialog box.

NOTE: For the conditions required to perform this operation and the instructions to start the installation program, refer the **Installation Maintenance** section located previously in this chapter.

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

To reinstall COMMANDCentral, follow these steps:

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

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

2. Click **Next** to begin the installation. The system displays the **Updating System** dialog box. Please wait while the program copies the COMMANDCentral 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 COMMANDCentral has been successfully installed.

3. Click **Finish** to exit.

REMOVING COMMANDCENTRAL

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

NOTE: For the conditions required to perform this operation and the instructions to start the installation program, refer the **Installation Maintenance** section located previously in this chapter.

2K/XP

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

To remove COMMANDCentral completely, follow these steps:

1. In the COMMANDCentral installation program's **Application Maintenance** dialog box, select **Remove**, and click **Next**. The system displays the **Uninstall** dialog box.
2. Click **Next** to remove COMMANDCentral. The system displays the **Updating System** dialog box. Please wait while the program removes the COMMANDCentral 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 COMMANDCentral has been successfully uninstalled.

3. Click **Finish** to exit.

8

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