

Command AntiVirus™
for
Microsoft® Exchange

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.**

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

**Published in the U.S.A. by Command Software Systems, Inc. All rights reserved.
Document No. CME-318-1003**

Part No. 07-1400-00b

TABLE OF CONTENTS

INTRODUCTION	1-1
Main Features	1-1
Chapter Overview	1-2
Chapter 1 - Introduction	1-2
Chapter 2 - Installation	1-2
Chapter 3 - Using Command AntiVirus	1-2
Chapter 4 - Automatic Update	1-2
Chapter 5 - Glossary	1-2
Appendix	1-2
Conventions Used	1-3
System Requirements	1-4
Additional Information	1-4
Web Site	1-4
Help Files	1-5
Mailing List Server	1-5
README.TXT	1-5
INSTALLATION	2-1
Installing	2-1
Getting Started	2-10
CSAV for Exchange Console	2-10
Removing Command AntiVirus	2-11
USING COMMAND ANTIVIRUS	3-1
The CSAV for Exchange Console	3-1
Task Window	3-2
About the Task List	3-2
Using the Console	3-5
Command Buttons	3-5
Shortcut Menus	3-6
MenuBar	3-7
Toolbar Buttons	3-7
Additional Ways to Access Program Features	3-8
Using the Quarantine Feature	3-9
Using the Task Menu	3-11
Creating a New Scan Task	3-12
Executing a Scan	3-12
Enable/Disable	3-14
Renaming a Scan Task	3-14
Deleting a Scan Task	3-14
Editing a Scan Task	3-15

Configuring Scanning Properties	3-16
Viewing Scan Statistics	3-48
Viewing the Log Files	3-51
Using the View Menu	3-53
Toolbar	3-53
Status Bar	3-54
Large Icons	3-54
Small Icons	3-54
List	3-54
Details	3-54
Refresh	3-54
Using the Tools Menu	3-55
CSAV Alerts	3-56
Virus Notification	3-58
Using Event Viewer	3-64
Outbreak Manager	3-66
Options	3-79
Help Menu	3-83
Index	3-83
Using Help	3-83
Technical Support	3-83
Error Report	3-83
About CSAV for Exchange	3-83
Configuring the MESSAGE.INI File	3-84
AUTOMATIC UPDATE	4-1
Preparing for the Automatic Update	4-1
Creating the Automatic Update Directory	4-1
Configuring the Automatic Update	4-3
Performing an Automatic Update	4-6
GLOSSARY	5-1
APPENDIX	A-1
Keyboard Shortcuts	A-1
Mail Alert Variables	A-2
CSAV Service Startup Options	A-4
INDEX	I-1



INTRODUCTION

This chapter provides an overview of Command AntiVirus™ for Microsoft® Exchange including a list of **Main Features**, **System Requirements**, and **Conventions Used** throughout this administrator's guide. It also contains details on accessing additional product-related information from the Command Software Systems web site.

MAIN FEATURES

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

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

CHAPTER OVERVIEW

The *Command AntiVirus for Microsoft Exchange Administrator's Guide* consists of the following chapters.

CHAPTER 1 - INTRODUCTION

This chapter provides an overview of CSAV including a list of features, conventions, and system requirements.

CHAPTER 2 - INSTALLATION

Chapter 2, *Installation*, covers the product's installation, uninstall, and reinstallation procedures.

CHAPTER 3 - USING COMMAND ANTIVIRUS

Chapter 3, *Using Command AntiVirus*, provides information on creating custom scans, setting scan properties, scheduling automatic scans, and configuring and using the Outbreak Manager. It also provides information on configuration settings, toolbar items, and menu bar options.

CHAPTER 4 - AUTOMATIC UPDATE

Chapter 4, *Automatic Update*, explains how to configure the automatic update feature. This feature allows your system to update itself with the latest Command AntiVirus program files and virus definitions.

CHAPTER 5 - GLOSSARY

Chapter 5, *Glossary*, provides definitions of virus terminology.

APPENDIX

The *Appendix* gives a complete listing of all the keyboard shortcuts that are available in CSAV. The appendix also provides information on service startup options and virus notification variables.

CONVENTIONS USED



Indicates an area that requires special attention.



Indicates a helpful tip.

COURIER

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

```
\\SERVER\SHARE\UPDATE
```

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 CSAV for Exchange, your system should meet the following minimum requirements:

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



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

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.authentium.com>
- Command Software UK – <http://www.authentium.co.uk>
- Command Software Australia – <http://www.commandcom.com.au>

HELP FILES

The Help files contain information that will assist you in using the product. You can obtain help by selecting **Help** from the **Help Menu** in the Command AntiVirus graphical user interface (GUI).

MAILING LIST SERVER

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

README.TXT

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



INSTALLATION

Installing Command AntiVirus™ (CSAV) for Microsoft® Exchange is a simple process. However, before installing the product, we recommend that you read this chapter. This will help you to make some of the setup choices during the actual installation procedure.

INSTALLING



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

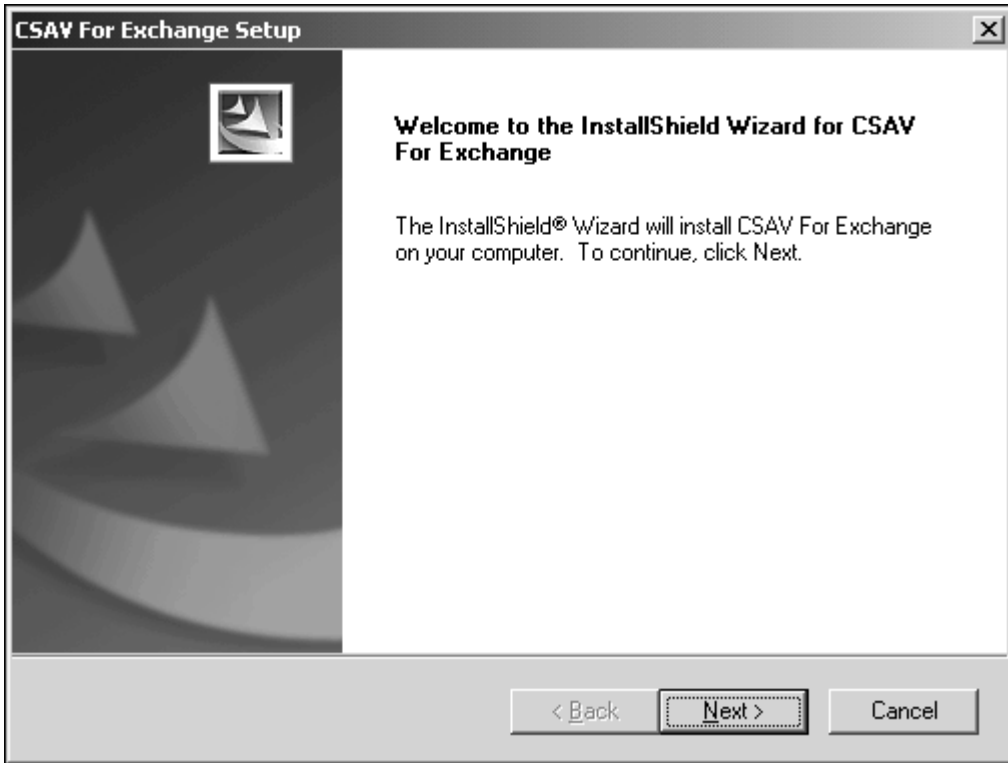
- Microsoft Exchange 2000 Server with SP1 or higher is running on your server.
- You are logged on as an administrator on the local domain.
- You remove any previous versions of Command AntiVirus for Exchange.
- You are **not** installing Command AntiVirus for Exchange through terminal services.



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

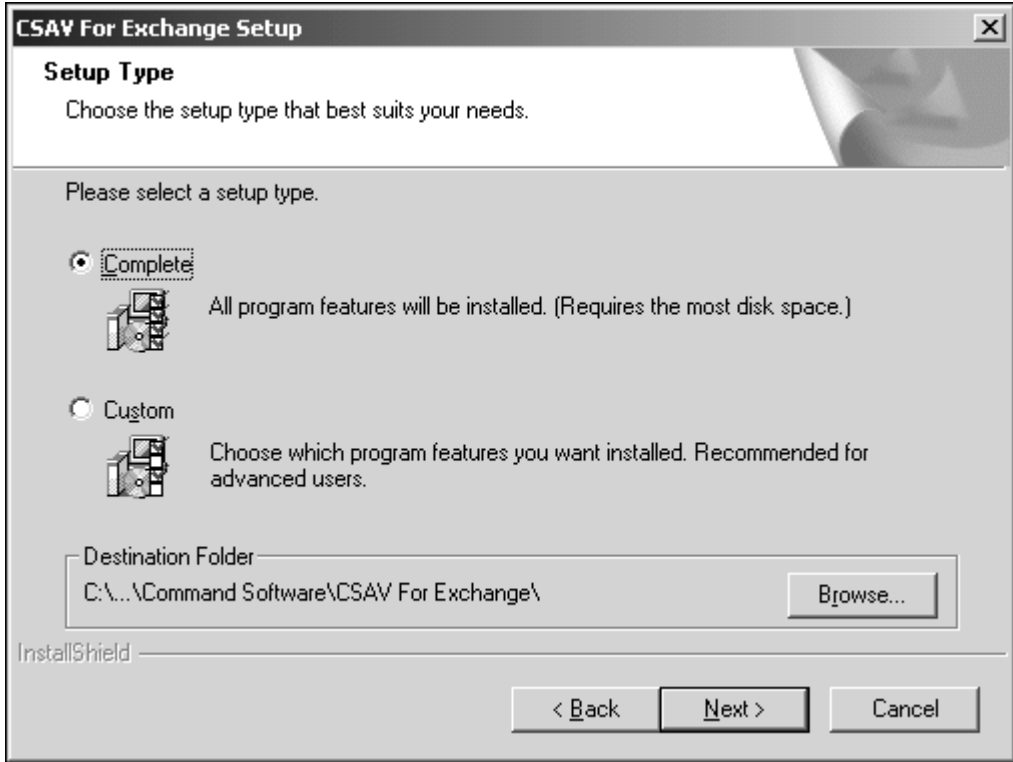
1. Insert the CD-ROM.
 2. On the taskbar, click the **Start** button.
 3. Click **Run**. The system displays the **Run** dialog box.
 4. Click **Browse** to search the CD for the **EXCHANGE** directory.
 5. Change to that directory.
-

6. Double-click **Setup.exe**, and click **OK**. After startup, the system displays the **Welcome** dialog box:



Welcome Dialog Box

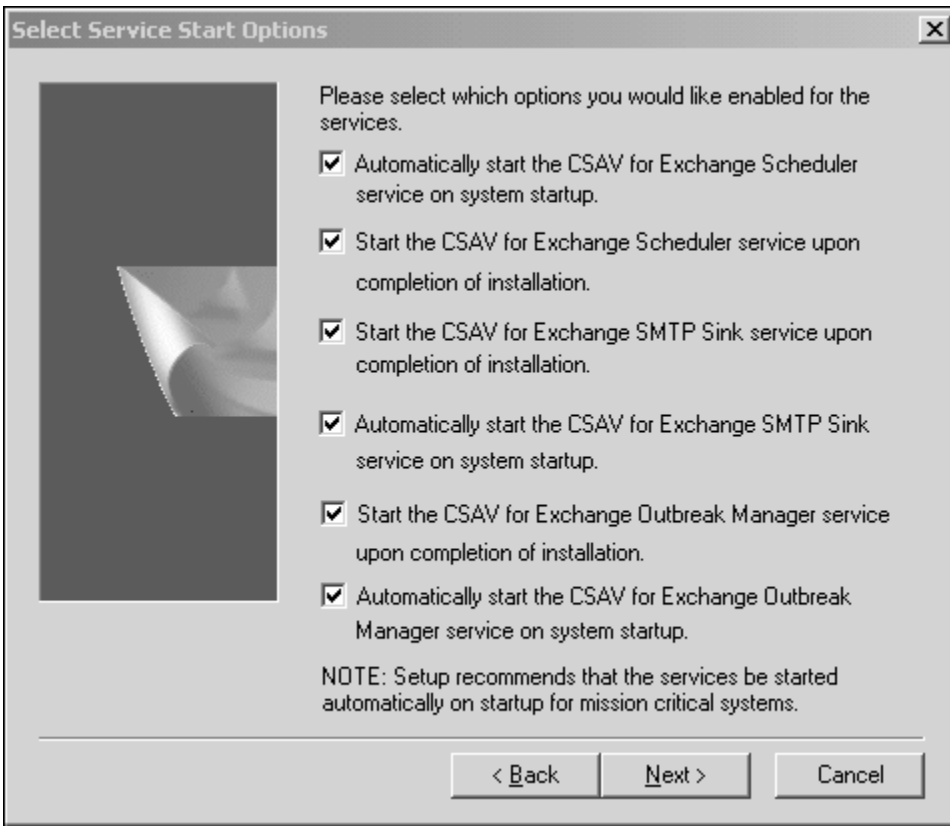
7. Click **Next**. The system displays the **Software License Agreement**.
8. To accept the license agreement, click **Yes**. The system displays the **Setup Type** dialog box:



Setup Type Dialog Box

9. Select **one** of the following installations. We recommend the **Complete** installation.
 - **Complete** – Installs all required files
 - **Custom** – Allows you to choose whether to install program files and help files
10. Specify the **Destination Folder** for the CSAV for Exchange files. You can accept the default destination folder or click the **Browse** button to select a different folder.

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



Select Service Start Options Dialog Box



NOTE: If you chose the **Custom** installation, the system first displays the **Select Features** dialog box. Select the features that you want to install and click **Next**.

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

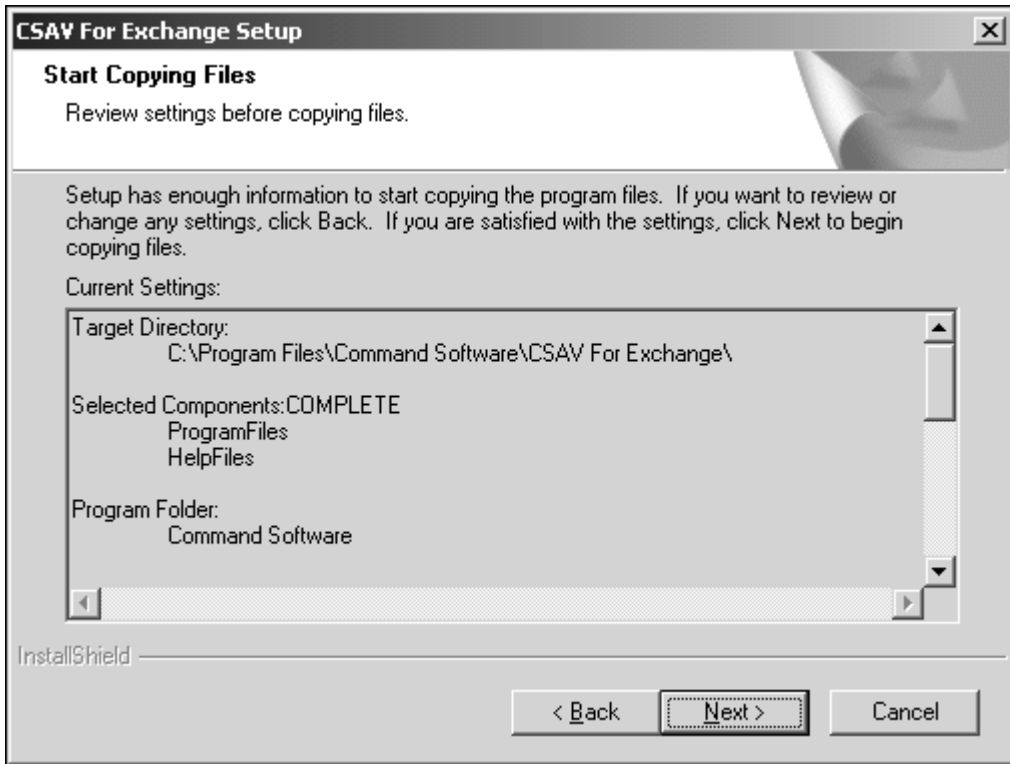
The **Scheduler** service allows you to schedule virus scans. The **SMTP Sink** service allows you to scan SMTP mail. SMTP mail includes mail that is sent over the Internet. The **Outbreak Manager** service allows you to define and configure rules to manage infected items received by the Exchange Server.

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



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

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



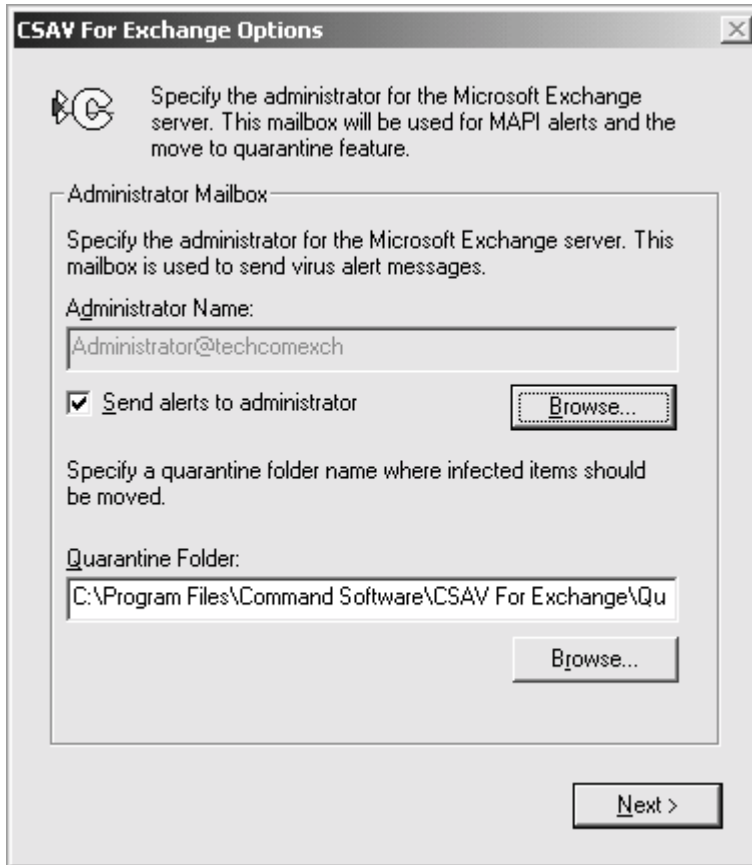
Start Copying Files Dialog Box



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

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

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



CSAV for Exchange Options Dialog Box

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

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

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



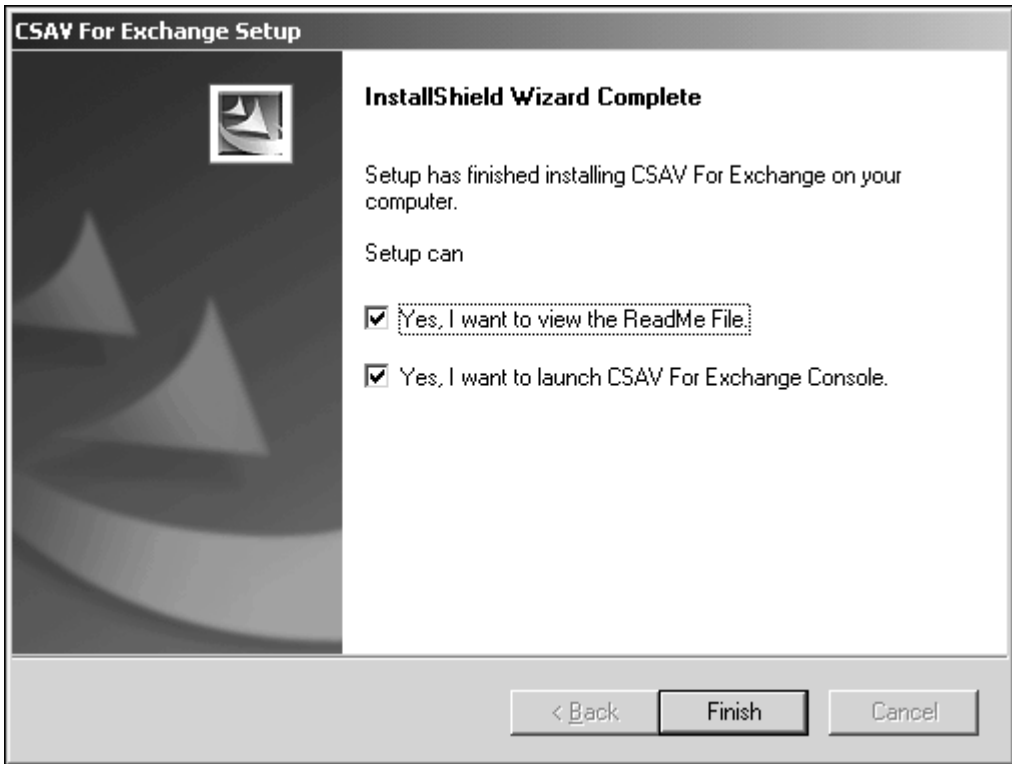
NOTE: You can also start or cancel sending a **mail alert message** from the **CSAV for Exchange Console** menu bar by clicking **Tools**, and then clicking **Options**. For more information, refer to [Options located on page 3-79](#) in the *Using Command AntiVirus* chapter of this guide.

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

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

For more information on the quarantine feature, refer to [Using the Quarantine Feature located on page 3-9](#) in the *Using Command AntiVirus* chapter of this guide.

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



Setup Complete Dialog Box

17. Select whether you want to view the **README** file and/or run the **CSAV for Exchange Console**. We recommend that you view the **README** file as it contains the latest information on the functionality of CSAV for Exchange.
 18. Click **Finish**. This completes the installation of CSAV for Exchange.
-

GETTING STARTED

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

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

CSAV FOR EXCHANGE CONSOLE

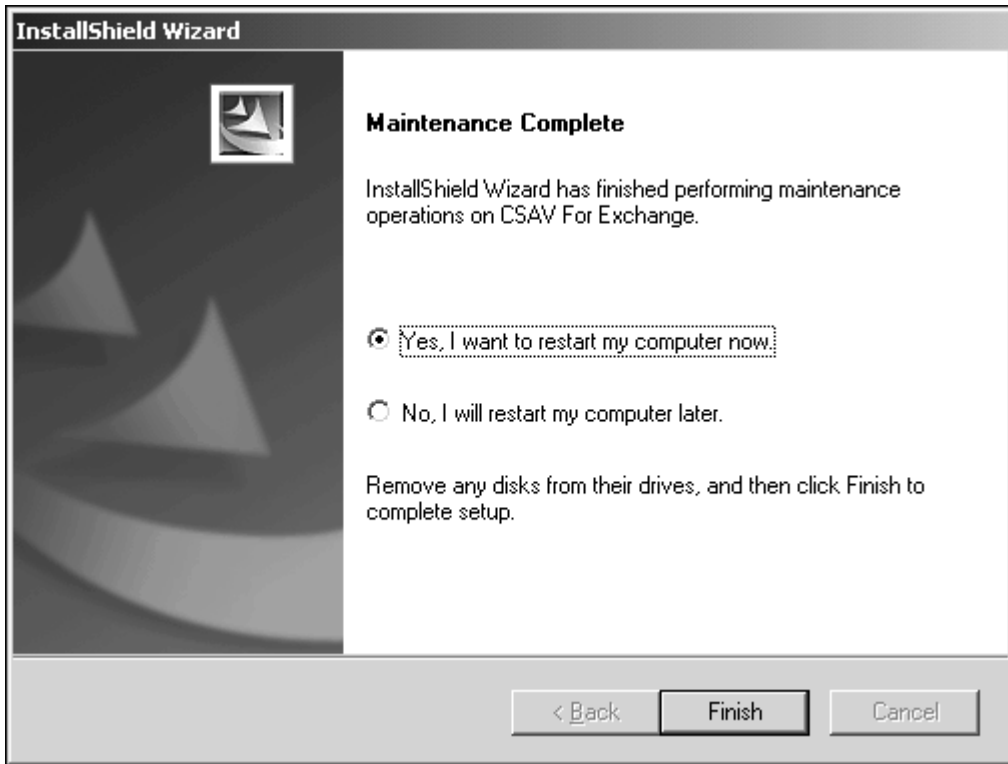
CSAV uses a graphical user interface (GUI) that simplifies the customizing and starting of virus scans. When you start CSAV for Exchange, the program displays the **CSAV for Exchange Console**.

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

REMOVING COMMAND ANTIVIRUS

To remove Command AntiVirus for Microsoft Exchange follow these directions.

1. On the Windows taskbar, click the **Start** button.
2. Select **Settings**.
3. Click **Control Panel**.
4. Double-click the **Add/Remove Programs** icon.
5. Select **CSAV for Exchange** from the list of installed applications.
6. Click the **Change/Remove** button. The uninstall wizard prepares for the uninstall and the system displays a message box asking if you want to completely remove CSAV for Exchange and all of its features.
7. Click **Yes**. When the uninstall completes, the system displays the **Maintenance Complete** dialog box:



Maintenance Complete Dialog Box

8. To restart your computer now, select **Yes, I want to restart my computer now**, and click **Finish**. To restart your computer at a later time, select **No, I will restart my computer later**, and click **Finish**.



You **must** restart your computer to completely remove CSAV for Exchange.

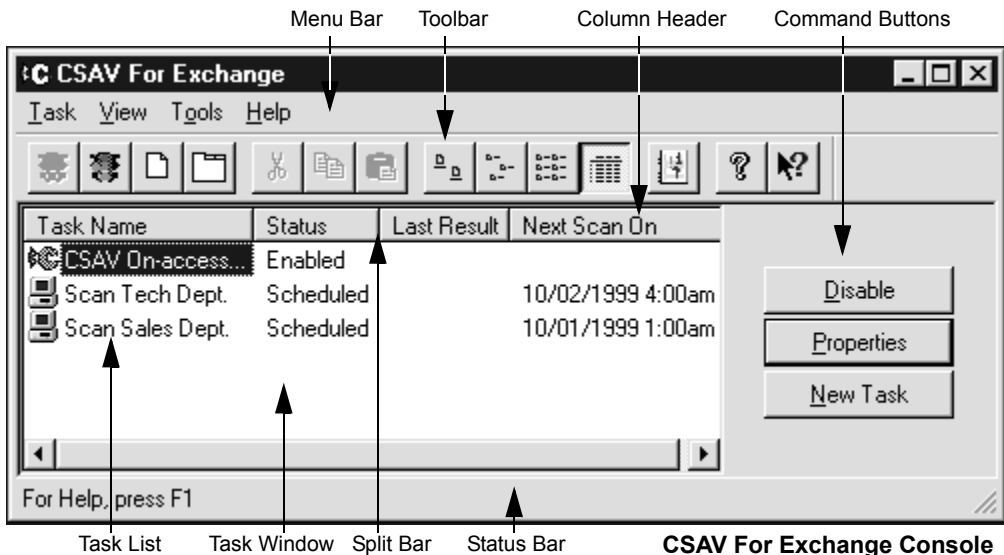


USING COMMAND ANTIVIRUS

Command AntiVirus (CSAV) for Microsoft® Exchange gives your network unbeatable security against virus-infected e-mail attachments. You can create customized scan tasks, schedule automatic scans, and specify which action CSAV takes when it finds a virus. The following sections describe the many features that allow you to modify Command AntiVirus to your specifications.

THE CSAV FOR EXCHANGE CONSOLE

CSAV for Exchange uses a graphical user interface (GUI) that simplifies the customizing and running of virus scans. The main screen of the GUI is called the **CSAV for Exchange Console**.



From the console, you can perform numerous scan task operations. For example, you can set the folder to which detected viruses are quarantined. You can also create, delete, modify, select, start, and enable/disable virus scans. The console also allows you to define and configure the **Outbreak Manager** to manage infected items received by the Exchange Server.

Configuring individual scan tasks is possible through the easy-to-use options found in the console's menu bar, toolbar or command buttons. A **Task List** in the console can be used to access all major configuration features for any individual scan task. For example, to change a scan's properties, highlight the scan task name in the **Task List** and click the **Properties** button. To turn the on-access (real-time) virus scanning on or off, select its scan task name in the **Task List**, click **Task** on the menu bar, and click **Enable** or **Disable**.

The console's menu bar contains **Task**, **View**, **Tools**, and **Help** menu items that you can use to configure Command AntiVirus or to find help on how to use the product's features.

TASK WINDOW

The main feature in the console is the **Task Window**. This window contains a **Task List** with **Task Names** identifying the available scan tasks. The **Status** column shows whether the on-access scan task is enabled/disabled or whether any on-demand tasks are scheduled to run automatically. The **Last Result** column shows the results of the last scan. The **Next Scan On** column shows the time of the next scheduled on-demand scan.

ABOUT THE TASK LIST

You can create and configure scan tasks from the **Task List**. For example, you can set properties for tasks and specify which actions to use upon detecting a virus. You can also create an activity log file, schedule scan tasks to run automatically and more.




Types of Scan Tasks

CSAV uses two types of scan tasks, on-access and on-demand. The on-access scan task runs continuously in the background. When CSAV for Exchange detects incoming or outgoing e-mail, the on-access scan takes place immediately. Because the scan takes place entirely in the background, it does not interrupt the workflow on your Exchange network.



NOTE: CSAV for Exchange can have only **one** on-access scan task. You cannot delete or schedule the on-access scan task. However, you can configure it to handle viruses according to your requirements.

On-demand scan tasks require that you start the scan manually. On-demand tasks scan e-mail attachments in folders and mailboxes upon request. You start an on-demand scan by selecting an on-demand scan task from the **Task List** and clicking the **Execute** button. You can create multiple on-demand scan tasks and configure each one to function according to your needs. On-demand scan tasks can be scheduled to start automatically. These are often referred to as scheduled scans.

Task Name	Status	Last Results	Next Scan On
 CSAV On Access Task	Enabled		
 Scan Marketing Mailboxes	Scheduled		09/19/1998 7:00pm
 Scan Suggestion Box	Scheduled		09/19/1998 12:00...

Task Window

In the **Task List**, the two types of scan tasks are identified by the icons appearing to the left of the scan task names. A computer icon indicates an on-demand scan. A yellow **C** icon identifies the on-access scan.

Sizing the Columns

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

Sort Order of Scan Tasks

You can sort scan tasks in the **Task List** by clicking the column headers. For example, clicking the **Last Results** header alphabetically sorts scan tasks that detected a virus. Clicking the **Task Name** header sorts scan tasks by their names.

Changing Icon Size of Scan Tasks

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

The **Large Icons** view displays the scan task names below their icons. The **Small Icons** view displays the scan task names to the right of the icons. These views do not show the results of the last scan conducted or the next scheduled scan time.

List or Details View of Scan Tasks

You can also view the **Task List** with or without details about each scan task. Selecting **List** from the **View** menu displays a column of small icons with scan task names to the right of the icons. Selecting **Details** displays a column of small icons with the scan task names to the right of the icons. The **Details** view also displays columns containing the results of the last scan and the time of the next scheduled scan. The **Details** view is the only viewing option that displays column headers.

Changing Scan Task Names

To change a scan task name, click its name in the **Task List**, pause, and click again. Then, type the new name for the scan task. You can also use the right mouse button (right-click) to click a scan task name and then select **Rename** from the shortcut menu. If you make an error while typing in a new scan task name, press the **Esc** key to go back to the original name.

USING THE CONSOLE

You can access CSAV for Exchange functions in numerous ways. From the **console**, you can use the command buttons, the menu bar, keyboard shortcuts or the toolbar to start scans or modify their properties.

COMMAND BUTTONS

The command buttons allow you to perform various scan task operations. Select the scan task you want to run or modify and then select the appropriate command button. For example, selecting an on-demand scan task and then clicking the **Execute** button starts an on-demand scan. Clicking the **Properties** button allows you to access the scan task configuration features.



Command Buttons



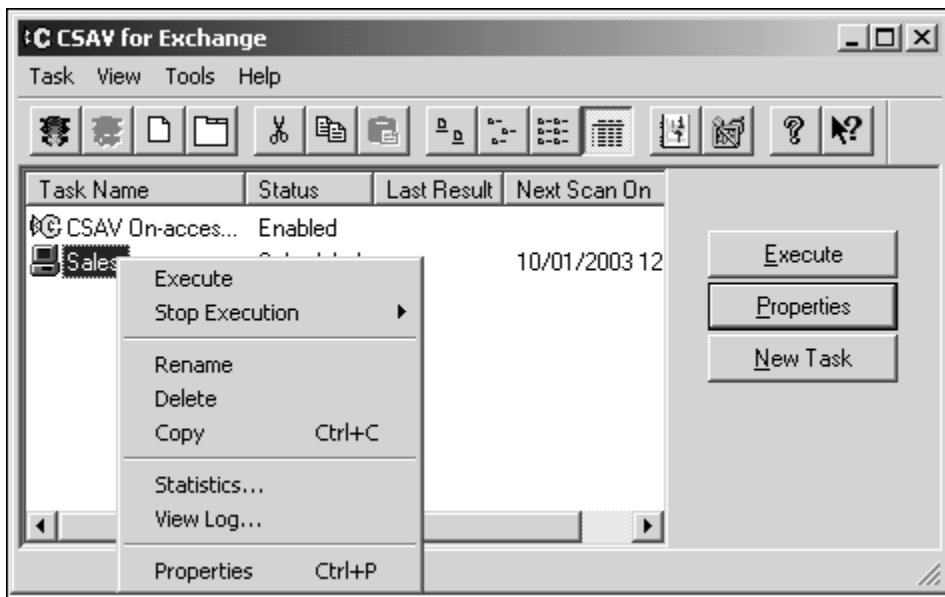
NOTE: If you select an on-demand scan task from the **Task List** the uppermost button is **Execute**. If you select the on-access scan task, the button is either **Enable** or **Disable** depending on the status of the on-access scan.

When you click the **New Task** button, the system prompts you for a new on-demand scan task name. After entering a name, click **Properties** to configure the task. After you complete the task's configuration, the new task is added to the **Task List**.

SHORTCUT MENUS

Shortcut menus allow you to create, start, rename, modify or delete a task entirely. They also contain other options to help you manage CSAV for Exchange. You can bring up a shortcut menu by using the right mouse button (right-click) to select any of the following:

- The on-access scan task
- An on-demand scan task
- Anyplace in the **Task Window** other than a task name



Shortcut Menu – On-demand Scan Task

The items available on a shortcut menu depend on what you select. For example, if you right-click the on-access scan task name, the system displays a shortcut menu containing **Enable/Disable**, **Statistics**, **View Log**, and **Properties**. If you right-click an on-demand scan task name, the system displays a shortcut menu containing **Execute**, **Stop Execution**, **Rename**, **Delete**, **Copy**, **Statistics**, **View Log**, and **Properties**. If you right-click anywhere in the **Task Window** other than

on a task name, the system displays a shortcut menu containing **New Task**, **Paste**, and **Options**.

If an item on a shortcut menu is **not** available, it appears dimmed.

MENUBAR

The menu bar in the **CSAV for Exchange Console** contains **Task**, **View**, **Tools**, and **Help** menus. These menus contain options allowing you to create, modify, delete or run scan tasks.

TOOLBAR BUTTONS

The toolbar provides quick access to functions that can also be accessed from other menus.



Toolbar Buttons



NOTE: You can move the mouse pointer over any toolbar button to display a ToolTip that identifies the function of that particular button.

From the **View** menu, you can turn on or turn off the toolbar as needed.

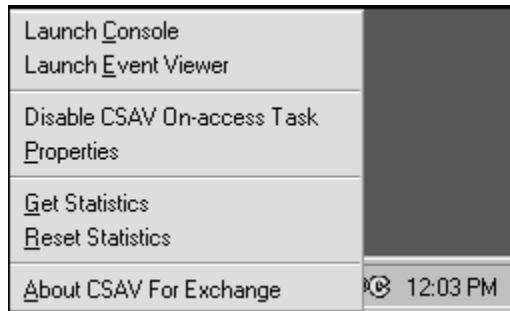
Help



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

ADDITIONAL WAYS TO ACCESS PROGRAM FEATURES


You can use the **C** icon in the notification area to the right of the taskbar to access the program quickly. If you double-click the icon, the system displays the **CSAV for Exchange Console**. If you right-click the icon, the system brings up the **CSAV Shortcut Menu**:

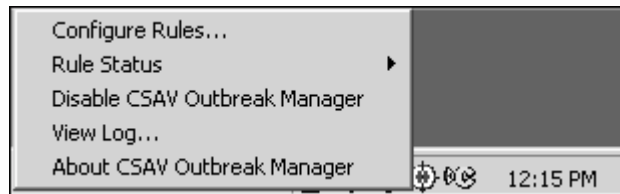


CSAV Shortcut Menu

The CSAV shortcut menu allows you to:

- Open the **CSAV for Exchange Console**
- Open the Windows® **Event Viewer**
- Enable or disable the on-access scan task
- Change the on-access scan task properties
- View on-access scan statistics
- Reset the information in the **Infected** list in the on-access **Statistics** dialog box
- View copyright and product version number information

You can use the **bull's-eye** icon  in the notification area to the right of the taskbar to access the **Outbreak Manager** service quickly. If you double-click the icon, the system displays the **CSAV Outbreak Rules** dialog box. If you right-click the icon, the system brings up the **Outbreak Manager Shortcut Menu**:



Outbreak Manager Shortcut Menu

The Outbreak Manager shortcut menu allows you to:

- Configure rules for **Outbreak Manager**
- View status for configured rules
- Enable or disable the **Outbreak Manager** service
- View the log file
- View copyright and product version number information

USING THE QUARANTINE FEATURE

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

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

By default, the file name of the new attachment contains the original file name with the **.VIRUS INFO.TXT** extension added to it.

For example, if the original file name and extension is **EICAR1.COM**, the name of the new attachment is:

```
EICAR1.COM.VIRUS INFO.TXT
```

You can customize the file name of the new attachment and the additional information message contained in it by editing the **MESSAGE.INI** file. For more information, refer to [Configuring the MESSAGE.INI File located on page 3-84](#).



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

For example, if the original file name and extension is **EICAR1.COM** and the virus name is **EICAR_TEST_FILE**, the name of the quarantined file is:

```
EICAR1.COM.EICAR_TEST_FILE.VIRUS
```

If this file name already exists, the name of the quarantined file is, for example:

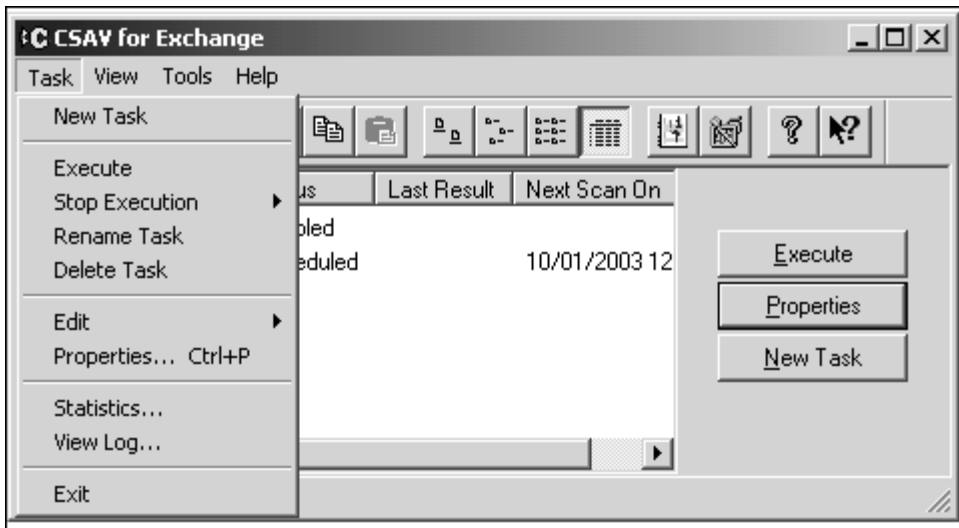
```
EICAR1.COM.EICAR_TEST_FILE.VIRUS.843
```

Before you can use the quarantine feature, you **must** specify a quarantine folder. For more information, refer to [Options located on page 3-79](#) in **Using the Tools Menu**.

To move infected files to the quarantine folder automatically, you must select the **Quarantine infected items automatically** option in the **Actions** dialog box. For more information, refer to [Action to Take on Infection located on page 3-26](#) in **Configuring Scanning Properties**.

USING THE TASK MENU

You can access the **Task** menu by clicking **Task** on the menu bar. The system displays the **Task Menu**:



Task Menu – On-demand Scan Task

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

- Create a **New Task**
- **Execute** an on-demand scan task
- **Enable/Disable** an on-access scan task
- **Stop Execution** of an on-access scan task
- **Rename** an on-demand scan task
- **Delete** an on-demand scan task
- Copy and paste tasks through the **Edit** item
- Modify the **Properties** of a scan task

- View the scan **Statistics** of executed tasks
- Examine the log files through **View Log**
- **Exit the CSAV for Exchange Console**

CREATING A NEW SCAN TASK

To create a new on-demand scan task, click **Task** on the menu bar. The system displays the **Task** menu. Click **New Task**. A new on-demand scan task called **New Scan Task** is created at the bottom of the **Task List**.

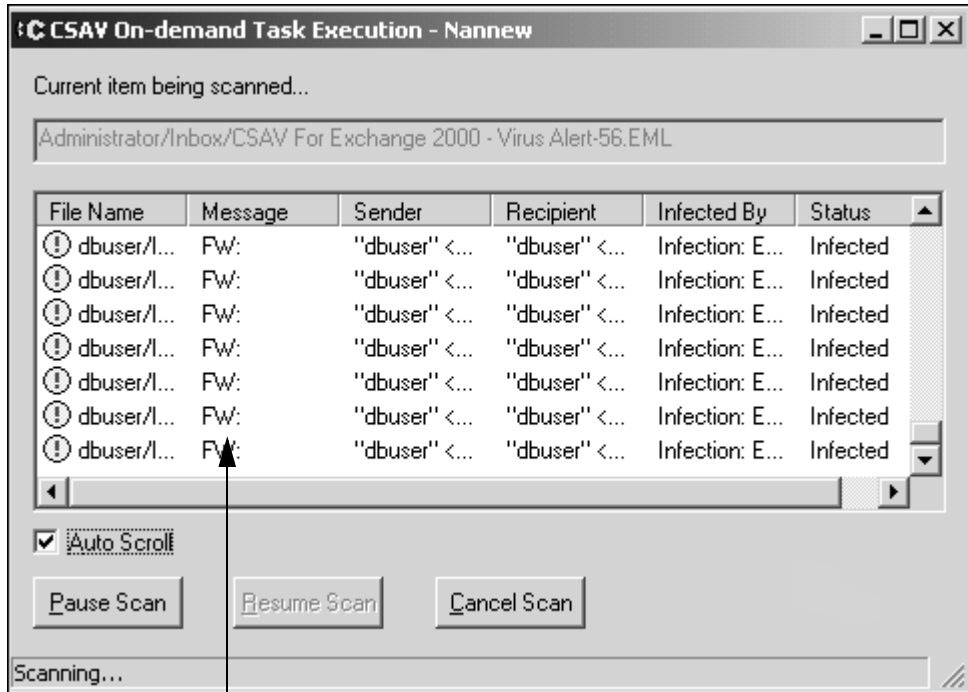
You can change the name of the new scan task by typing in the new name and pressing **Enter** to save the change.

To configure the scanning characteristics of the scan task, select the scan task name from the **Task List**. Click **Task** on the menu bar and then click **Properties**.

For more information, refer to [Configuring Scanning Properties](#) located on page 3-16.

EXECUTING A SCAN

To start an on-demand scan, select an on-demand task from the **Task List**. Click **Task** on the menu bar, and then click **Execute**. The system displays the **CSAV On-demand Task Execution** dialog box and starts the scan immediately.



Task Execution Window

CSAV On-demand Task Execution Dialog Box

The name of the scan task appears in the title bar of the dialog box.

The **Current item being scanned** text box displays the names of the files being scanned. As files are scanned in real-time, the names displayed in this text box change quickly.

The **Task Execution Window** displays the following:

- **File Name** – Contains the addresses of any infected files. If you cannot see the full path for a file in **File Name**, use your mouse to drag the right or left border of the **File Name** column header until you can see the full path.
- **Message** – Contains the subject of the message that was scanned.

- **Sender** – Contains the names of the individuals who sent the messages.
- **Recipient** – Contains the names of the individuals who received the messages.
- **Infected By** – Lists the names of the viruses that are infecting the e-mail files.
- **Status** – Reports what action CSAV for Exchange performed on the infected files.

The **On-demand Task Execution** dialog box also contains the following buttons:

- **Pause Scan** – Suspends the current scan.
- **Resume Scan** – Continues the scan from the spot at which it was paused.
- **Cancel Scan** – Ends the current scan before all items targeted by the scan have been scanned.

ENABLE/DISABLE

To start or stop the on-access scan task, select the on-access task in the **Task List**. Click **Task** on the menu bar and then click either **Enable** or **Disable**.

RENAMING A SCAN TASK

To rename a scan task, select the task's name in the **Task List**. Click **Task** on the menu bar and then click **Rename Task**. Type the new name of the scan task and press **Enter**.

DELETING A SCAN TASK

To delete a scan task, select the task name from the **Task List**. Click **Task** on the menu bar and then click **Delete Task**.



NOTE: The on-access scan task is a permanent feature in CSAV. It can be configured, but it cannot be renamed or deleted.

EDITING A SCAN TASK

The **Edit** menu item allows you to **Copy** and **Paste** scan tasks in the **Task List**.

If you use the **Copy** item, be sure to modify the properties of the new scan task so that they do not duplicate the properties of the task from which it was created.

To copy an on-demand scan task named **Scan Marketing Inbox**, for example, follow these steps:

1. In the **Task List**, click **Scan Marketing Inbox**.
2. On the menu bar, click **Task**. The system displays the **Task** menu.
3. Select **Edit**. The system displays a submenu.
4. Click **Copy**.
5. On the menu bar, click **Task**.
6. Select **Edit**. The system displays a submenu.
7. Click **Paste**. A new scan task named **Scan Marketing Inbox1** is created in the **Task List**. If more than one copy is made, the following copies have a sequential number. For example, **Scan Marketing Inbox2**, **Scan Marketing Inbox3**.
8. Type in the new name of the scan task.
9. Press **Enter** to save the change.

You can then modify the new scan task's properties. For more information, refer to [Configuring Scanning Properties](#) located on page 3-16.



NOTE: As there can be only one on-access scan task. You cannot cut, copy or paste the on-access scan task.

CONFIGURING SCANNING PROPERTIES

If you select **Properties** from the **Task** menu, the system displays the **Properties** dialog box. This dialog box contains several other dialog boxes. For on-demand scans, the available dialog boxes are **Detection**, **Actions**, **Reports**, **Schedule**, and **Exclusion**. For on-access scans, the available boxes are **Detection**, **Actions**, **Advanced**, and **Reports**. Each of these dialog boxes is identified by a name tab. When you click a tab, the system displays the dialog box referenced by the tab. For example, clicking the **Actions** tab displays the **Actions** dialog box.

Each scan task must have its properties individually configured. The following sections provide instructions on how to use the **Detection**, **Actions**, **Advanced**, **Reports**, **Schedule**, and **Exclusion** dialog boxes to configure the on-access scan and on-demand scans.

Detection Options

The **Detection** dialog box provides the option to scan the body of an e-mail message and to select which mailboxes, folders, and types of attachments to scan.

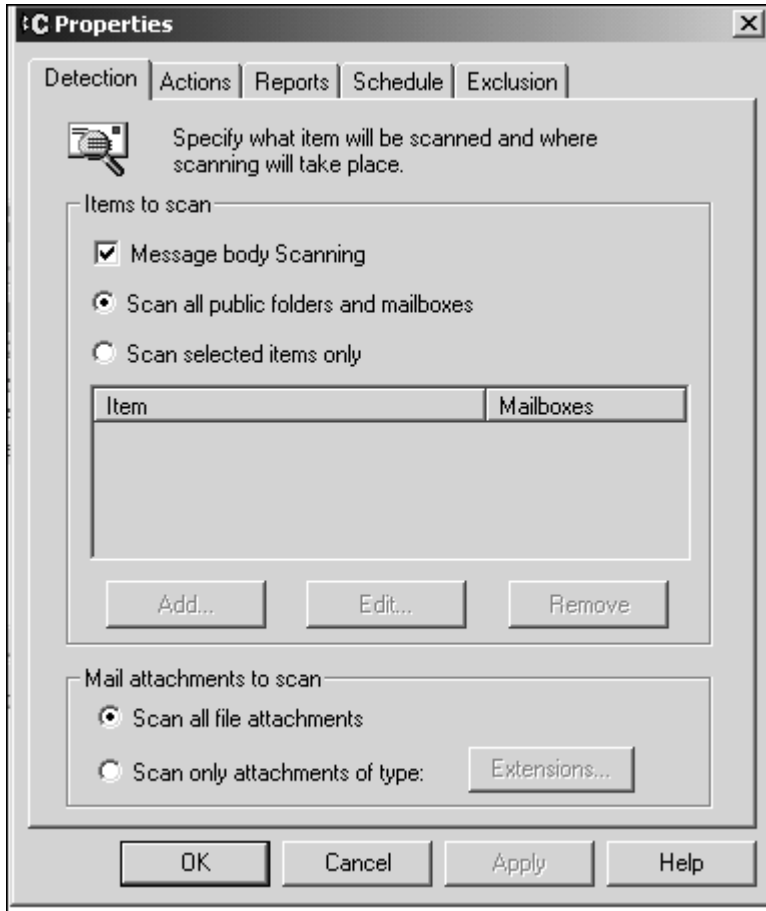


If some objects selected for a scan in the **Detection** dialog box are the same as those selected in the **Exclusion** dialog box, these objects are excluded from scanning. This is because the **Exclusion** dialog overrides the **Detection** dialog for the same items.

On-demand Scan Tasks

To configure the detection properties for an on-demand scan task, follow these steps:

1. Select an on-demand scan task from the **Task List**.
2. Click **Task** on the menu bar. The system displays the **Task** menu.
3. Click **Properties**. The system displays the **Properties** dialog box with the **Detection** dialog box in view:



Detection Dialog Box – On-demand Scan Task

4. Under **Items to scan**, select from the following options:
 - **Message body Scanning** – Scans the body of an e-mail message. This option is selected by default.



We highly recommend that you do **not** clear this check box.



NOTE: Select only one of the following options:

- **Scan all public folders and mailboxes** – Scans all of the Exchange mailboxes and folders. If you select this option, go to **Step 8**.
- **Scan selected items only** – Adds, edits, and removes mailbox and folder locations from the list of items to be scanned. Selecting this option activates the **Add** button.

5. To add an item to the scan, click **Add**. The system displays the **Browse Exchange Folders** dialog box:

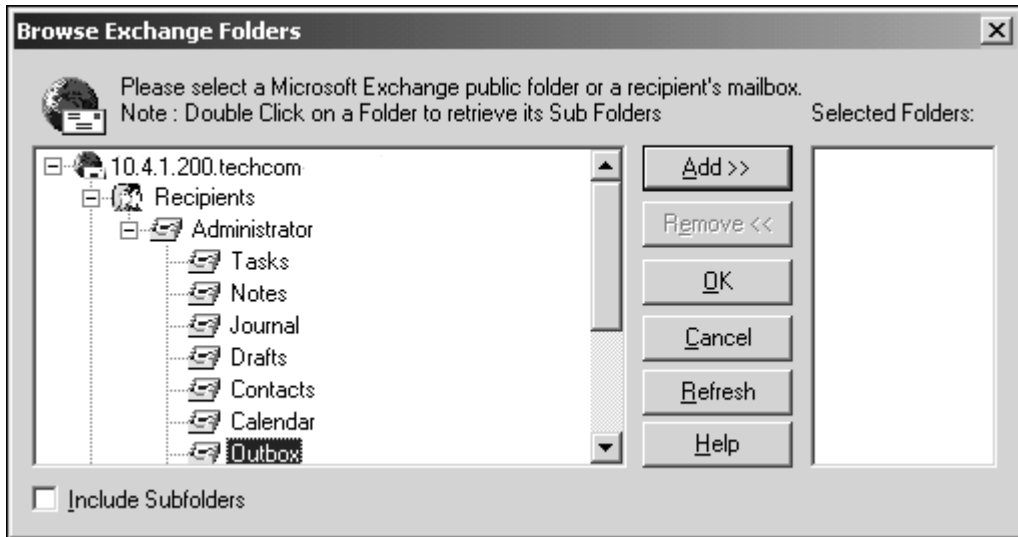


NOTE: You can use the **Edit** and **Remove** buttons in the **Items to scan** group box to edit and remove items listed in the **Item** column.



Browse Exchange Folders Dialog Box

6. In the **Browse Exchange Folders** dialog box, select the folder(s) or recipient mailbox(es) that you want the task to scan. Click the plus sign (+) located to the left of **Recipients** and **Folders** to expand these items.



Browse Exchange Folders Dialog Box – Expanded View



NOTE: To select multiple single files and/or folders, click the file or folder, hold down the **Ctrl** key, and then click each file or folder that you want to select.

To select a block of files and/or folders, click the first file or folder in the block, hold down the **Shift** key, and then click the last file or folder in the block.

- **If you select a folder** – the **Include Subfolders** check box is selected by default. To turn off this option, clear the **Include Subfolders** check box.



NOTE: If you select **Folders**, the **Include Subfolders** check box is permanently selected by default. You **cannot** clear this check box.

- **If you select a recipient** – you can select which mailboxes (**Inbox**, **Outbox**, **Deleted Items**, **Sent Items**) are to be included in the scan. This feature allows you to select different subfolders for each recipient mailbox. The **Include Subfolders** check box is selected by default. To turn off this option, clear the **Include Subfolders** check box.

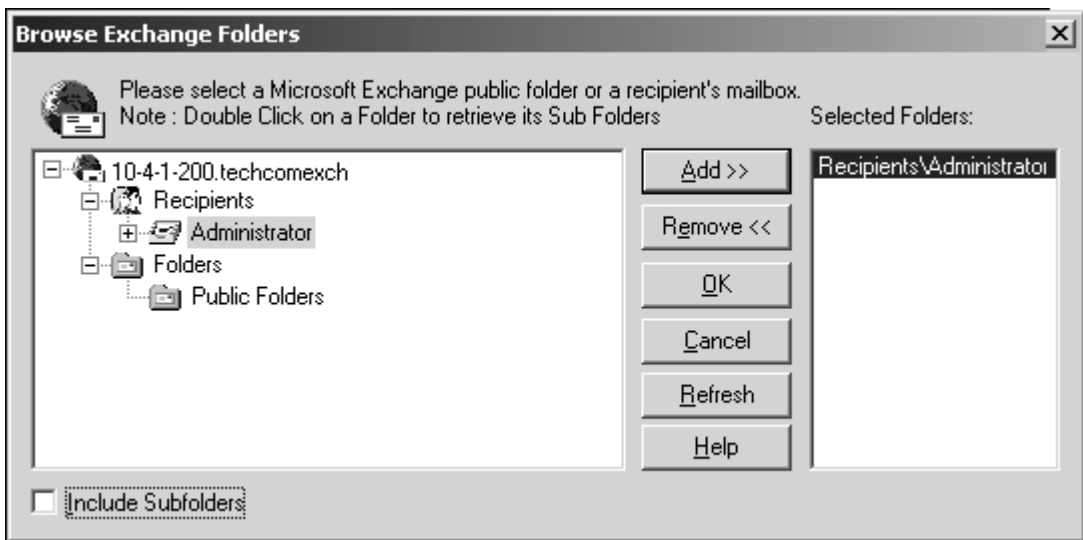


NOTE: If you select **Recipients**, the **Include Subfolders** check box is permanently selected by default. You **cannot** clear this check box.

7. Click **Add**. The system adds the selected folder or recipient to the **Selected Folders** list.



NOTE: To remove a folder or recipient from the **Selected Folders** list, select the folder or recipient, and click **Remove**.



Browse Exchange Folders Dialog Box

8. Click **OK**. The system returns the **Detection** dialog box. The folder or recipient mailbox that you selected is now in the **Items to Scan** list.

9. Under **Mail attachments to scan**, select one of the following:

- **Scan all file attachments** – Scans file attachments of all types (that is *.*). This is the default option. If you select this option, go to **Step 12**.



NOTE: We highly recommend that you select the default option, **Scan all file attachments**.

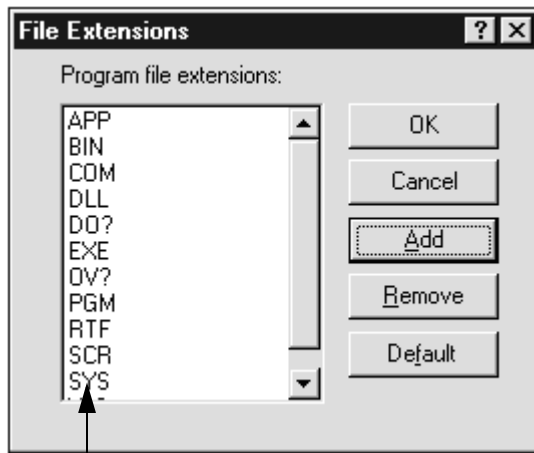
- **Scan only attachments of type** – Allows you to specify a list of attachment types, for example, file extensions, that CSAV will scan. Attachment types are identified by their file extensions. Click the **Extensions** button to display the **File Extensions** dialog box.



Scan only attachments of type option provides coverage for only those files with extensions listed in the **File Extensions** dialog box. If you select this option, we recommend that you add the **ZIP, AR?, JAR, CAB, PKG, RAR, LZH, LHA, TAR, TGZ, ACE, and GZ** extensions to the file extensions list.



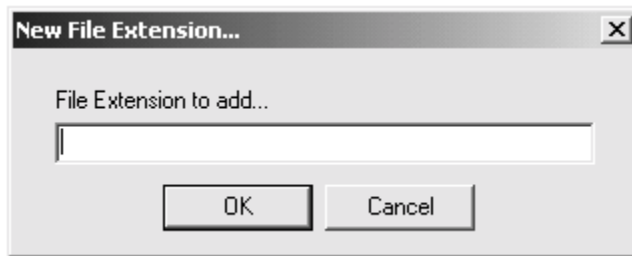
NOTE: To provide the most up-to-date antivirus protection, the default extensions in the file extension list may change from version to version.



File Extensions List **File Extensions Dialog Box**

10. In the **File Extensions** dialog box, use the following instructions to add or remove an extension from the file extensions list:

To add a file extension, click **Add**. The system displays the **New File Extension** dialog box:



New File Extension Dialog Box

- Type the three-character extension of the file type you want to add to the file extensions list, for example, SED. Click **OK** to return to the **File Extensions** dialog box. The extension is displayed in the contents of the file extensions list.
 - To remove a file extension, in the **File Extensions** dialog box, select the extension you want to remove and click the **Remove** button. The extension is immediately removed from the file extension list. Repeat this process if you want to remove any additional extensions.
11. Click **OK**.
 12. In the **Detection** dialog box, click **OK** to save your changes.



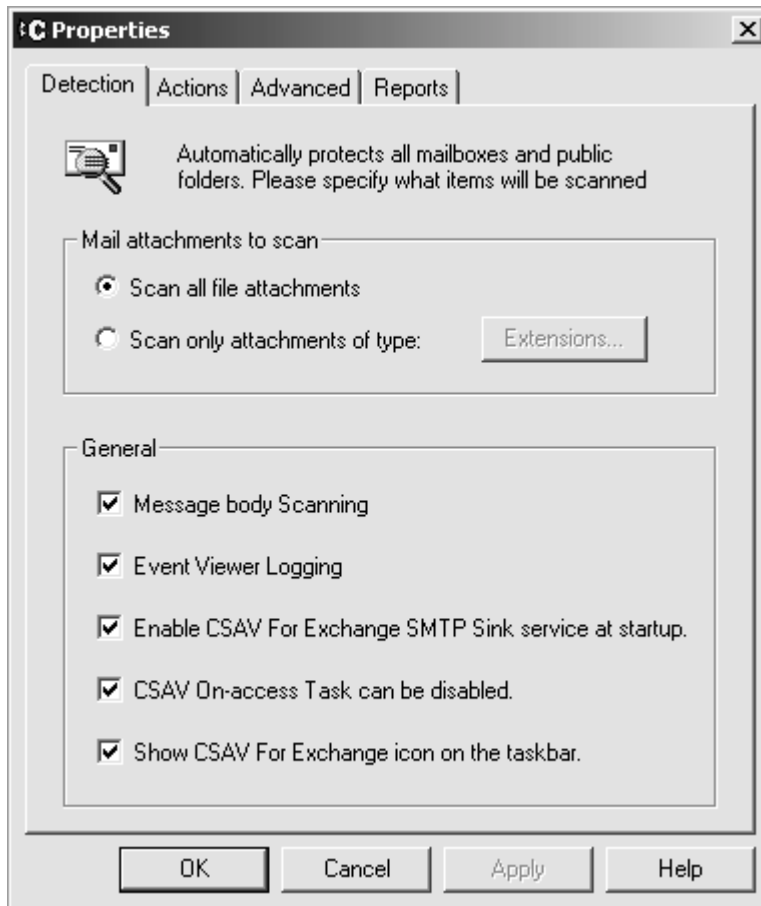
The **Default** button in the **File Extensions** dialog box resets the list to the default extensions. Any file extensions you added are lost.

On-access Scan Task

The detection options for the on-access scan task differ from those available for on-demand scan tasks. Both types of scan tasks have a **Mail attachments to scan** group box with identical options. However, the **Detection** dialog box for the on-access scan task has a **General** group box instead of an **Items to scan** group box.

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

1. In the **Task List**, select the on-access scan task.
2. On the menu bar, click **Task**. The system displays the **Task** menu.
3. Click **Properties**. The system displays the **Properties** dialog box with the **Detection** dialog box in view:



Detection Dialog Box – On-access Scan Task

4. Under **Mail attachments to scan**, select **one** of the following:

- **Scan all file attachments** – Scans file attachments of all types (that is *.*). This is the default option. If you select this option, go to **Step 8**.



NOTE: We highly recommend that you select the default option, **Scan all file attachments**.

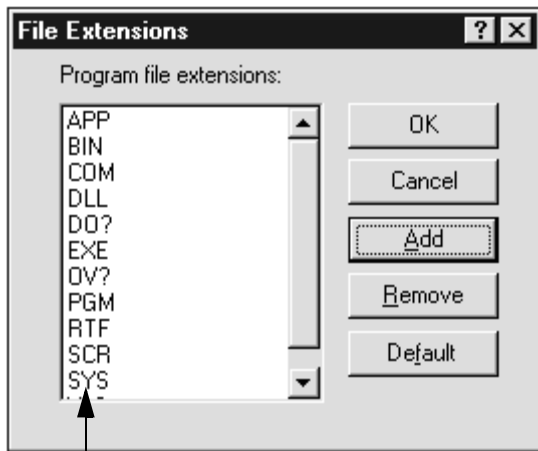
- **Scan only attachments of type** – Allows you to specify a list of attachment types, for example, file extensions, that CSAV will scan. Attachment types are identified by their file extensions. Click the **Extensions** button to display the **File Extensions** dialog box.



The **Scan only attachments of type** option provides coverage for only those files with extensions listed in the **File Extensions** dialog box. If you select this option, we recommend that you add the **ZIP, AR?, JAR, CAB, PKG, RAR, LZH, LHA, TAR, TGZ, ACE, and GZ** extensions to the file extensions list.



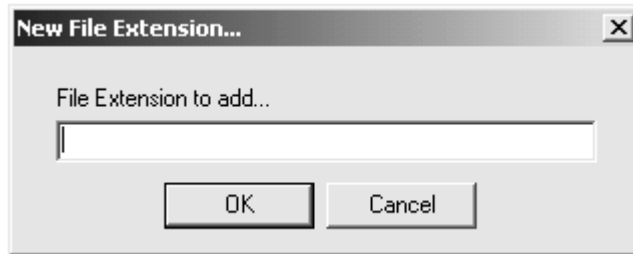
NOTE: To provide the most up-to-date antivirus protection, the default extensions in the file extension list may change from version to version.



File Extensions List **File Extensions Dialog Box**

5. In the **File Extensions** dialog box, use the following instructions to add or remove an extension from the file extensions list:

To add a file extension, click **Add**. The system displays the **New File Extension** dialog box:



New File Extension Dialog Box

- Type the three-character extension of the file type you want to add to the file extensions list, for example, SED. Click **OK** to return to the **File Extensions** dialog box. The extension is displayed in the contents of the file extensions list.
 - To remove a file extension, in the **File Extensions** dialog box, select the extension you want to remove and click the **Remove** button. The extension is immediately removed from the file extension list. Repeat this process if you want to remove any additional extensions.
6. Click **OK**.
 7. In the **General** group box, all of the following options are selected by default:

We highly recommend that **all** of these options remain selected.



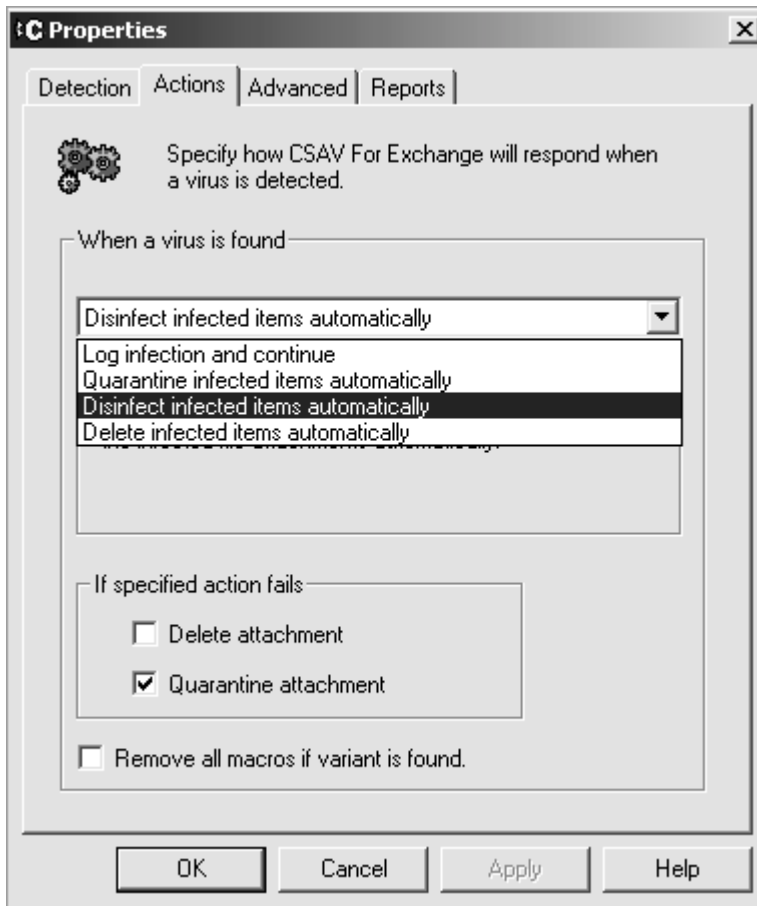
- **Message body Scanning** – Scans the body of e-mail messages.
- **Event Viewer Logging** – Allows you to view monitoring and troubleshooting messages from CSAV.

- **Enable CSAV For Exchange SMTP Sink service at startup** – Allows you to scan SMTP mail. SMTP mail includes mail that is sent over the Internet.
 - **CSAV On-access Task can be disabled** – If selected, allows users at the server running CSAV for Exchange to turn off the on-access scan task. The on-access scan task can then be disabled (or reenabled) using the **Enable/Disable** command that is available from the **CSAV for Exchange Console**. Disabling the on-access scan task stops automatic scanning of new mail that is received or sent.
 - **Show CSAV for Exchange icon on the taskbar** – Displays the yellow **C** icon in the notification area to the right of the taskbar. Clear this option if you do not want users at the server running CSAV for Exchange to access the program through the icon.
8. Click **OK** to save your changes.

Action to Take on Infection

The **Actions** dialog box allows you to specify the action to be taken when a virus is detected. To specify an action, follow these steps:

1. In the **Task List**, select a scan task.
2. On the menu bar, click **Task**. The system displays the **Task** menu.
3. Click **Properties**. The system displays the **Properties** dialog box.
4. Click the **Actions** tab. The system displays the **Actions** dialog box:



Actions Dialog Box

5. In **When a virus is found**, click the drop-down-arrow and select **one** of the following actions:
 - **Log infection and continue** – Records information about the infected attachments to a log file and continues the scanning process.
 - **Quarantine infected items automatically** – Moves virus-infected attachments to the quarantine folder.

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

By default, the file name of the new attachment contains the original file name with the extension **.VIRUS INFO.TXT** added to it.

For example, if the original file name and extension is **EICAR1.COM**, the name of the new attachment is:

```
EICAR1.COM.VIRUS INFO.TXT
```

You can customize the file name of the new attachment and the additional information message contained in it by editing the **MESSAGE.INI** file. For more information, refer to [Configuring the MESSAGE.INI File located on page 3-84](#).



NOTE: When an infected file is moved to the **Quarantine** folder, it is renamed. For more information, refer to [Using the Quarantine Feature located on page 3-9](#).

- **Disinfect infected items automatically** – Disinfects attachments. The attachments are disinfecting without any manual intervention. This is the default setting. If an on-demand scan uses this option, the disinfected attachment is reattached to the e-mail message.

If you select this option, the **Remove all macros if variant is found** option at the bottom of the dialog box is also selected by default. This option removes all macros from the infected attachment if a variant of an existing macro virus is found. If you do not want all macros to be removed if a variant is found, clear this check box.

- **Delete infected items automatically** – Deletes the infected attachments without any manual intervention.



Use the **Delete infected items automatically** option with care. Automatically deleting infected attachments can result in the loss of important information or data.

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

By default, the file name of the new attachment contains the original file name with the extension **.VIRUS INFO.TXT** added to it.

For example, if the original file name and extension is **EICAR1.COM**, the name of the new attachment is:

```
EICAR1.COM.VIRUS INFO.TXT
```

You can customize the file name of the new attachment and the additional information message contained in it by editing the **MESSAGE.INI** file. For more information, refer to [Configuring the MESSAGE.INI File located on page 3-84](#).

6. If you selected **Log infection and continue**, click **OK** to save your **Action** settings. Otherwise, proceed to the next step.
7. Depending on the action that you selected in **When a virus is found**, one, both or none of the following options are available in **If specified action fails**. Select only **one** option. If **Quarantine attachment** is available, it is the default. Select the option that you want.
 - **Delete attachment** – If the **Disinfect infected items automatically** or **Quarantine infected items automatically** actions fail, enabling this option assures that the infected e-mail object is not received by a user. This option deletes the infected attachments without any manual intervention.



Use the **Delete attachment** option with care. Automatically deleting infected attachments can result in the loss of important information or data.

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

By default, the file name of the new attachment contains the original file name with the extension **.VIRUS INFO.TXT** added to it.

For example, if the original file name and extension is **EICAR1.COM**, the name of the new attachment is:

```
EICAR1.COM.VIRUS INFO.TXT
```

You can customize the file name of the new attachment and the additional information message contained in it by editing the **MESSAGE.INI** file. For more information, refer to [Configuring the MESSAGE.INI File located on page 3-84](#).

- **Quarantine attachment** – If the **Disinfect infected items automatically** action fails, enabling this option assures that the infected e-mail object is not received by a user. This option moves virus-infected attachments to the quarantine folder.

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

By default, the file name of the new attachment contains the original file name with the extension **.VIRUS INFO.TXT** added to it.

For example, if the original file name and extension is **EICAR1.COM**, the name of the new attachment is:

```
EICAR1.COM.VIRUS INFO.TXT
```

You can customize the file name of the new attachment and the additional information message contained in it by editing the **MESSAGE.INI** file. For more information, refer to [Configuring the MESSAGE.INI File located on page 3-84](#).



NOTE: When an infected file is moved, it is renamed. For more information, refer to [Using the Quarantine Feature located on page 3-9](#).

8. Click **OK** to save your **Action** settings.

Advanced Settings for On-access scan task

The **Advanced** dialog box allows you to configure the following:

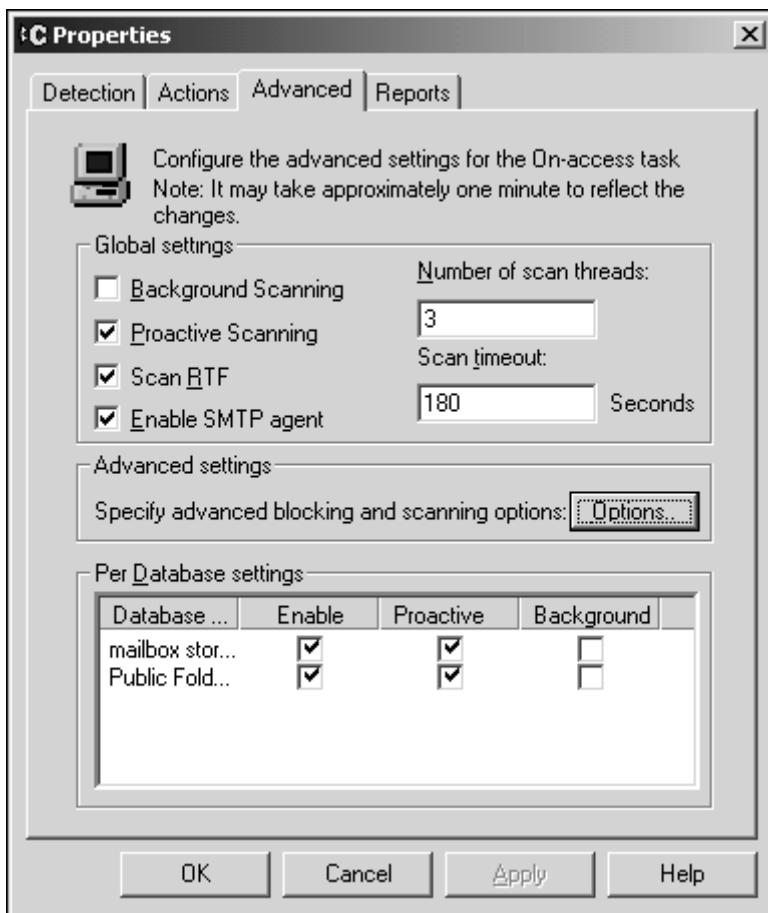
- Memory to be used for scanning
- Mail types to be scanned
- Maximum amount of time a thread has to access a message before the scan times out
- Mail messages to be blocked from delivery



We highly recommend that only experienced administrators configure these options.

To configure the advanced settings, follow these steps:

1. In the **Task List**, select the on-access scan task.
2. On the menu bar, click **Task**. The system displays the **Task** menu.
3. Click **Properties**. The system displays the **Properties** dialog box.
4. Click the **Advanced** tab. The system displays the **Advanced** dialog box:



Advanced Dialog Box

5. Under **Global settings** select one of the following two scanning options:
 - **Background Scanning** – Uses any available memory for scanning. This setting conserves memory usage.
 - **Proactive Scanning** – Creates its own memory space to use for scanning.



NOTE: The following two options are selected by default. We highly recommend that you do **not** change these selections.

- **Scan RTF** – Scans RTF formatted mail.
 - **Enable SMTP agent** – Scans SMTP mail. SMTP mail includes mail that is sent over the Internet.
6. Under **Global settings** in the **Scan timeout** text box, type the maximum amount of time a thread has to access a message before the scan times out. We recommend the default value of 180 seconds.
 7. Under **Advanced settings**, click the **Options** button to specify the mail messages that you want to stop from being delivered. The system displays the **Options** dialog box:



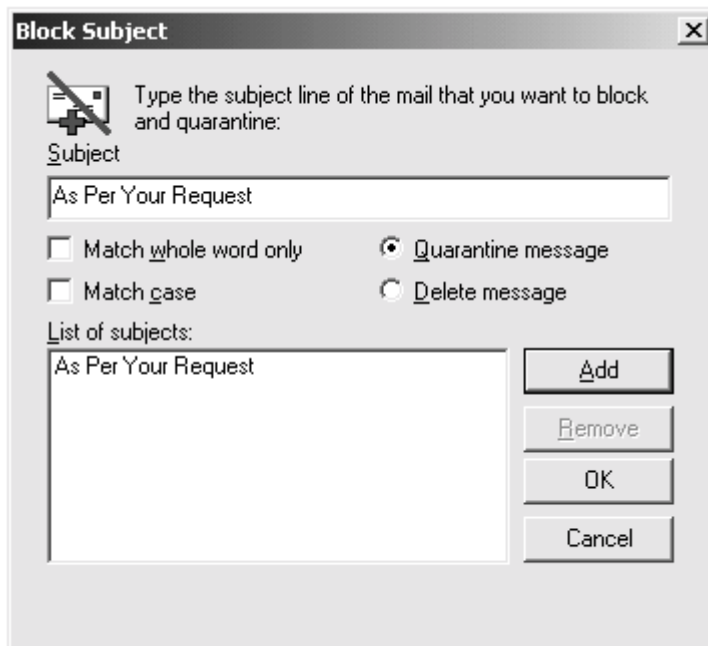
Options Dialog Box

The **Options** dialog box allows you to block the message based on the subject line, file name, and/or file extension. This dialog box also allows you to scan or block fragmented messages, and to specify if the blocked message should be quarantined or deleted.

Message Blocking

If you want to block messages based on the subject line, file name, and/or file extension, select from the following options:

- **Block Subject** – Allows you to specify the subject line of mail that is suspected of containing a virus. Selecting this option activates the **Subject** button. Click **Subject**. The system display the **Block Subject** dialog box:



Block Subject Dialog Box

To block messages that contain a specific subject line, follow these steps:

- A. In the **Subject** text box, type the subject line of mail that you want to block, and click **Add**. The subject is added to the **List of subjects**.



NOTE: To remove a subject, in the **List of subjects**, select the subject, and click **Remove**.

B. Select one or both of the following check boxes:

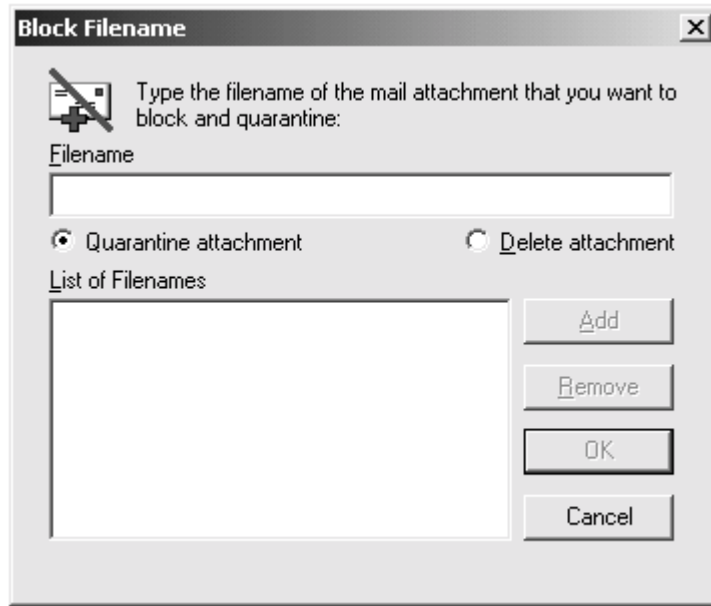
- **Match whole word only** – Matches the **Subject** by the entire subject line and **not** by individual words.
- **Match case** – Matches the **Subject** by how it is typed, for example, upper or lower case.

C. Select **one** of the following buttons:

- **Quarantine message** – Quarantines the message when a message is blocked.
- **Delete message** – Deletes the message when a message is blocked.

D. Click **OK**.

- **Block File** – Allows you to specify the file name of mail attachments that are suspected of containing a virus. Selecting this option activates the **Filename** button. Click **Filename**. The system displays the **Block Filename** dialog box:



Block Filename Dialog Box

To block messages that contain a specific file name, follow these steps:

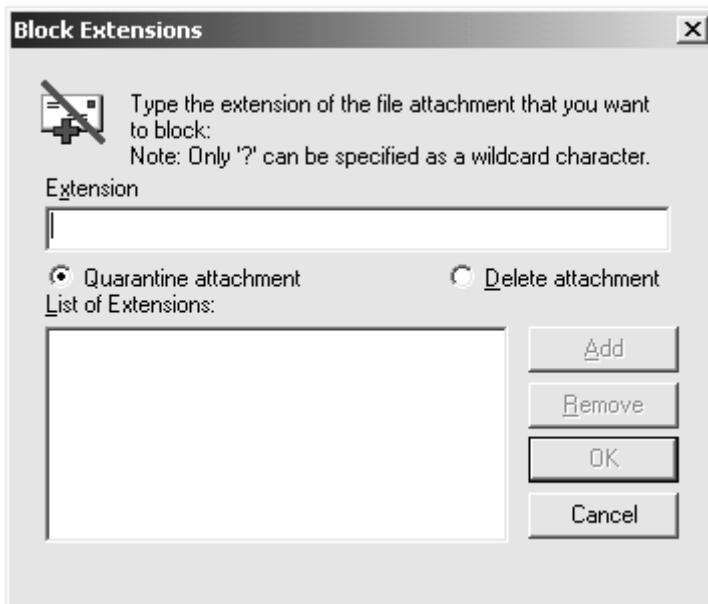
- A. In the **Filename** text box, type the file name of the attachment that you want to block, and click **Add**. The file name is added to the **List of Filenames**.



NOTE: To remove a file name, in the **List of Filenames**, select the file name, and click **Remove**.

- B. Select one of the following buttons:
 - **Quarantine message** – Quarantines the message when a message is blocked.
 - **Delete message** – Deletes the message when a message is blocked.

- C. Click **OK**.
- **Block Extension** – Allows you to specify the extension of file attachments that are suspected of containing a virus. Selecting this option activates the **Extension** button. Click **Extension**. The system displays the **Block Extensions** dialog box:



Block Extensions Dialog Box

To block messages that contain a specific file extension, follow these steps:

- A. In the **Extension** text box, type the extension of the file attachment that you want to block and click **Add**. The extension is added to the **List of Extensions**.



NOTE: To remove an extension, in the **List of Extensions**, select the extension, and click **Remove**.

B. Select **one** of the following buttons:

- **Quarantine message** – Quarantines the message when a message is blocked.
- **Delete message** – Deletes the message when a message is blocked.

C. Click **OK**.

Fragmented Message Scanning

If you want to scan or block fragmented messages, follow these steps:

A. select **one** of the following buttons:

- **Scan fragmented (partial) messages** – Allows you to scan fragmented messages suspected of containing a virus.
- **Block fragmented (partial) messages** – Allows you to block fragmented messages suspected of containing a virus.

B. Select **one** of the following buttons:

- **Quarantine attachment** – Quarantines the message when a fragmented message is blocked.
- **Delete attachment** – Deletes the message when a fragmented message is blocked.

C. Click **OK**.

8. The **Per Database settings** group box displays a list of Exchange databases and the current status of the following settings. You can also change these settings from this group box.



NOTE: If you right-click anywhere in the **Per Database settings** list, the system displays a menu that allows you to **Select All** or **Clear All** settings.

- **Enable** – allows you to enable or disable the on-access scan task.

- **Proactive** – Creates its own memory space to use for scanning.
 - **Background** – Uses any available memory for scanning. This setting conserves memory usage.
9. Click **OK** to save your settings.

Reports

In the **Reports** dialog box, you can specify the information to include in a scan task's activity log file. The default log file for the on-access scan task is **CSAVOnAccess.log**. The default log file for on-demand scan tasks is **CSAVOnDemand.log**. Activity log files are stored in the **CSAV for Exchange** installation folder. The latest scan information is appended to the end of the scan task's log file.

By specifying a different file name, in the **Log to file** text box, during the report setup procedure, you can save a report to a file other than the default file. To view a report for a scan task, select the scan task from the **Task List**. On the menu bar, click **Task**. The system displays the **Task** menu. Click **View Log** to display the log. In addition, log files can be viewed with any standard text editor.

To customize a scanning report for a task, follow these steps:

1. In the **Task List**, select a scan task name.
2. On the menu bar, click **Task**. The system displays the **Task** menu.
3. Click **Properties**. The system displays the **Properties** dialog box.
4. Click the **Reports** tab. The system displays the **Reports** dialog box:



Reports Dialog Box

5. Select the **Log to file** option to save a report to a log file. You can use the default file name shown or click **Browse** to bring up the **Select activity log file** dialog box.
6. Select **Limit size of log file to** and set the size to fit your requirements. The default size is **100KB**; the minimum is **10 KB**; the maximum is **999 KB**.

7. In **What to log**, select the types of information that you want logged:
 - **Infected items detected** – Reports how many viruses were detected
 - **Infected items disinfected** – Reports the number of attachments that were disinfected
 - **Date and time** – Reports the date and time of the scan operation
 - **Infected items deleted** – Reports the number of infected attachments that were deleted during scanning (depends on the action selected for the scan task)
 - **Infected items quarantined** – Reports the number of infected attachments that were moved to the quarantine folder (depends on the action selected for the scan task)
 - **User name** – Reports the name of the user logged into the Windows 2000 Server system running CSAV for Exchange
8. Click **OK** to save your changes.

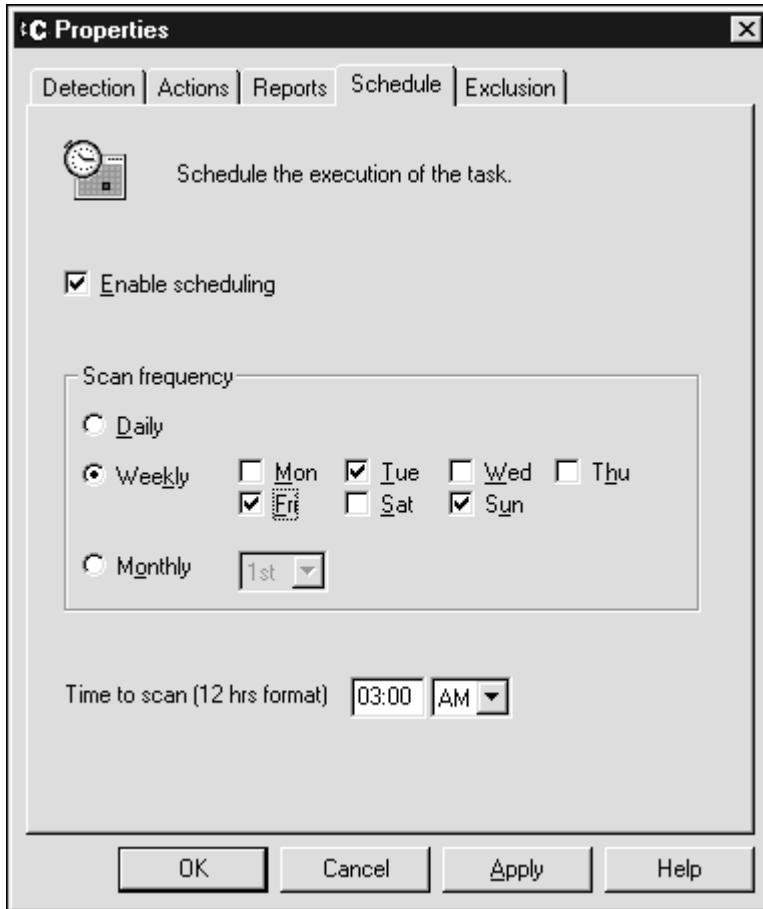
Scheduling Scans

You can configure on-demand tasks to perform scans automatically at a scheduled date and time. The **CSAV for Exchange Console** does not need to be open for scheduled scans to start. Through the **Properties** dialog box, administrators can assign a schedule to any on-demand scan task. Only on-demand scan tasks can be scheduled.

If **Details** is selected in the **View** menu, the **Task Window** displays the status for an on-demand scan task. For example, if the scan task is scheduled to run, the **Status** column shows **Scheduled**. The date and time of the scan are shown in the **Next Scan On** column.

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

1. In the **Task List**, select an on-demand scan task.
2. On the menu bar, click **Task**. The system displays the **Task** menu.
3. Click **Properties**. The system displays the **Properties** dialog box.
4. Click the **Schedule** tab. The system displays the **Schedule** dialog box:



Schedule Dialog Box – On-demand Scan Task

5. Select the **Enable scheduling** option.
6. Specify the **Scan frequency** by selecting one of the following:
 - **Daily** – Runs once every day.

- **Weekly** – Runs on one or more days of the week. Select the days you want the scan task to run.
 - **Monthly** – Runs on a specified date once every month. Click the drop-down arrow to select a date.
7. After you have selected a **Daily**, **Weekly** or **Monthly** scan frequency, use the **00:00** format to specify the time of day for the scans to start. In the **Time to scan (12 hrs format)** box, type the hour and minutes. Click the down arrow to select **AM** or **PM**.
 8. Click **OK** to finish.



NOTE: The on-access scan task cannot be scheduled. It can only be enabled or disabled. This option is located on the **Task** menu.

Excluding Specific Folders or Recipients from Scans

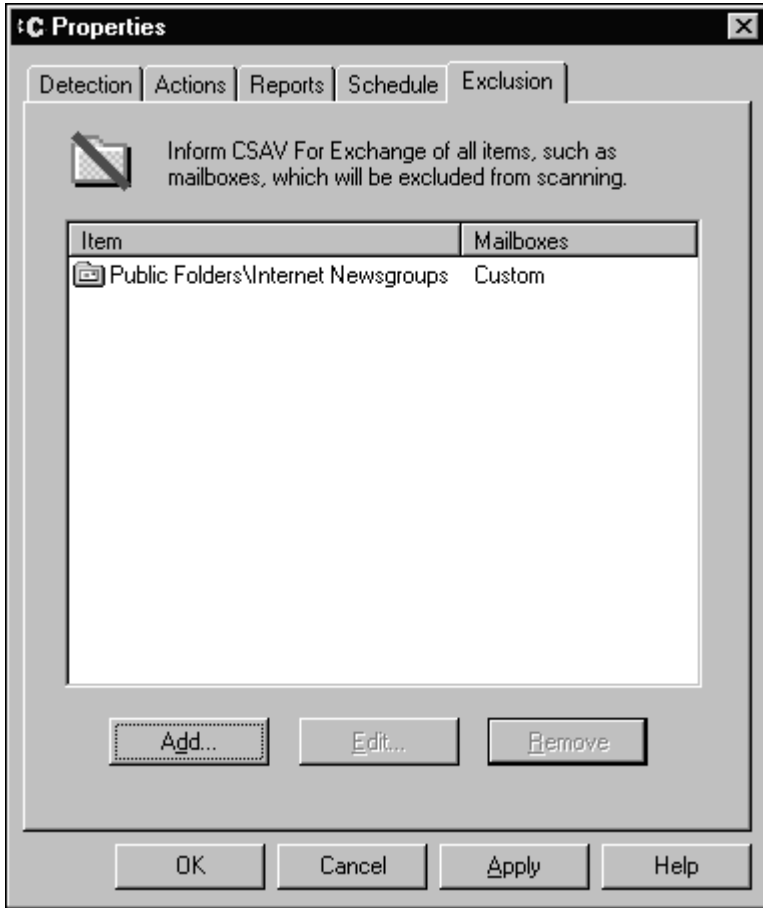
The **Exclusion** dialog box allows you to specify the folders and/or recipient mailboxes that you want to exclude from on-demand scans. For example, you can exclude the **Outbox** and **Sent Items** folders of a specific mailbox.



If some of the items selected for scanning in the **Detection** dialog box are the same as those in the **Exclusion** dialog box, those items will be excluded from virus scans.

To exclude specific folders or recipients from an on-demand scan task, follow these steps:

1. In the **Task List**, select an on-demand scan task.
2. On the menu bar, click **Task**. The system displays the **Task** menu.
3. Click **Properties**. The system displays the **Properties** dialog box.
4. Click the **Exclusion** tab. The system displays the **Exclusion** dialog box:

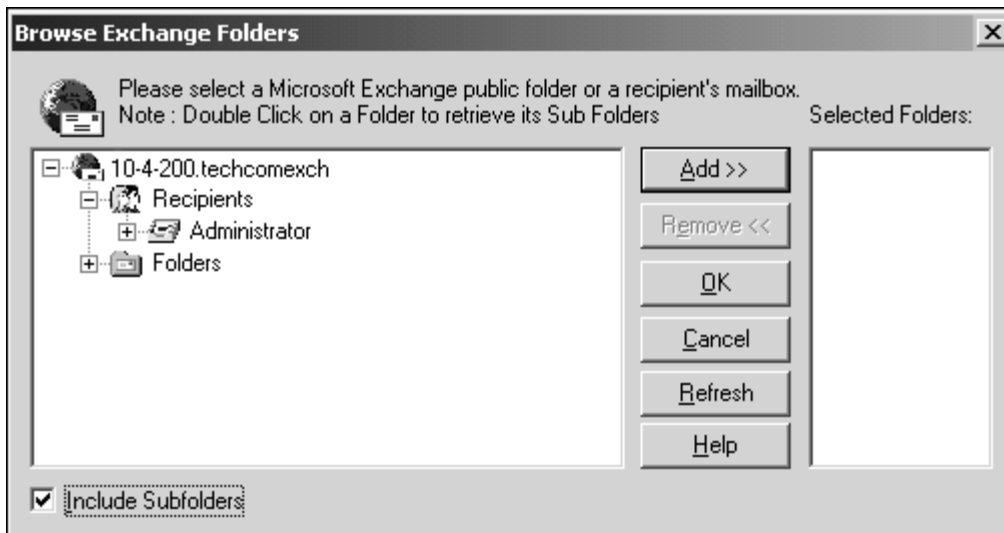


Exclusion Dialog Box – On-demand Scan Task

- Click the **Add** button. The system displays the **Browse Exchange Folders** dialog box.

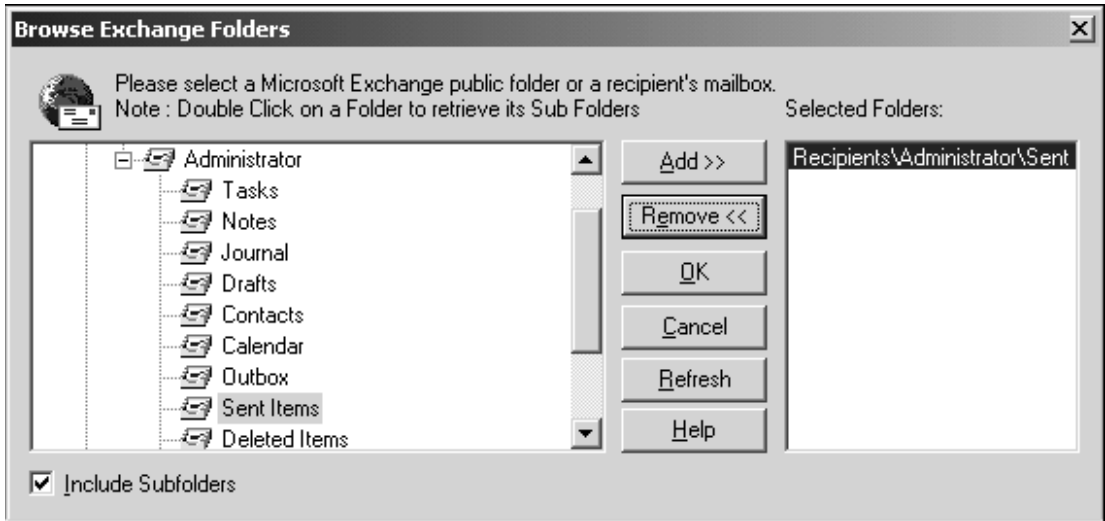


NOTE: You can use the **Edit** and **Remove** buttons to edit and remove items listed in the **Item** column.



Browse Exchange Folders Dialog Box

- In the **Browse Exchange Folders** dialog box, select the folder(s) or recipient mailbox(es) that you want the task to exclude from the scan. Click the plus sign (+) located to the left of **Recipients** or **Folders** to expand these items.



Browse Exchange Folders Dialog Box



NOTE: To exclude **all** folders, select **Folders**. To exclude **all** recipients, select **Recipients**. If you select **Folders** or **Recipients**, the **Include Subfolders** check box is permanently selected by default. You **cannot** clear this check box.

To select multiple single files and/or folders, click the file or folder, hold down the **Ctrl** key, and then click each file or folder that you want to select.

To select a block of files and/or folders, click the first file or folder in the block, hold down the **Shift** key, and then click the last file or folder in the block.

- **If you select a folder** – the **Include Subfolders** check box is selected by default. To turn off this option, clear the **Include Subfolders** check box.
- **If you select a recipient** – you can select which mailboxes (**Inbox**, **Outbox**, **Deleted Items**, **Sent Items**) are to be excluded from the scan. This feature allows you to select different subfolders for each recipient mailbox. The **Include Subfolders** check box is selected by default. To turn off this option, clear the **Include Subfolders** check box.

7. Click **Add**. The system adds the selected folder or recipient mailbox to the **Selected Folders** list.



NOTE: To remove a folder or recipient from the **Selected Folders** list, select the folder or recipient and click **Remove**.

8. Click **OK**. The system returns to the **Exclusion** dialog box. The folder or recipient mailbox selected for exclusion appears in the **Exclusion** list.

You can repeat the process for other folders or recipient mailboxes.

VIEWING SCAN STATISTICS

The **Statistics** menu item allows you to view the results of a scan.

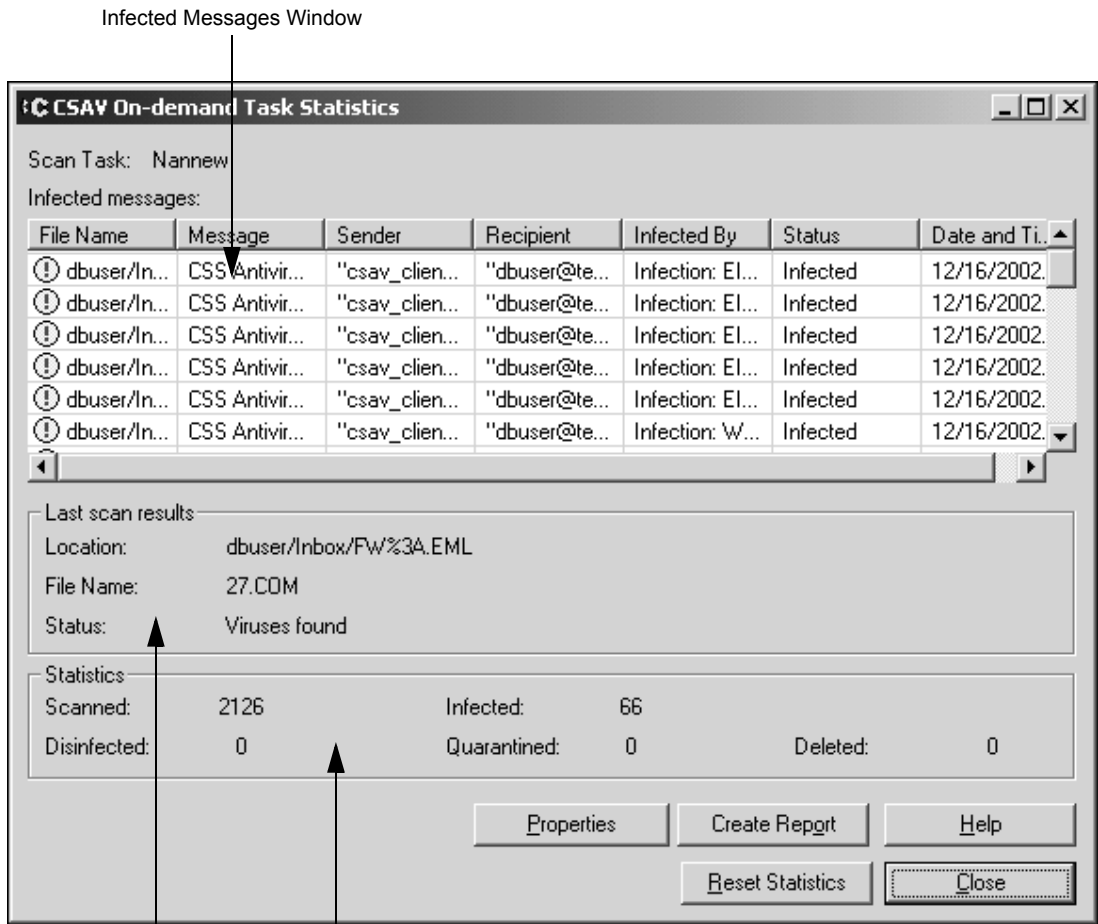
To view the statistics for a scan task:

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



NOTE: You can also view scan task statistics by right-clicking a scan task name in the **Task List** and then clicking the **Statistics** item on the shortcut menu.

For the on-access scan task, the system displays the **CSAV On-access Task Statistics** dialog box. For on-demand scan tasks, the system displays the **CSAV On-demand Task Statistics** dialog box:



Task Statistics Dialog Box – On-demand Scan Task

Last Scan Results Group Box

Statistics Group Box

The **Infected Messages** window in the **CSAV On-demand Task Statistics** dialog box displays the name of the folder in which an infected file was detected. The name of the infected file appears at the end of the folder's directory path.

The **Infected Messages** window also displays the name of the infected e-mail message, the sender's name, recipient's name, the type of virus that infected the message, the CSAV status of the message, and the date and time of the scan.



NOTE: The **CSAV On-access Task Statistics** dialog box contains an **Infected messages** window that displays only the name of the infected file, the type of virus that infected the message, the CSAV status of the message, and the date and time of the scan.

The lower portion of the **Statistics** dialog box displays the **Last Scan Results** group box. This box contains information indicating the location of the last folder and last file scanned. The **Status** line indicates whether a virus was found during the last scan.

The **Statistics** group box contains information on how many files were scanned, disinfected, infected, and deleted. The group box also reports the number of files that were moved to the quarantine folder.



NOTE: The counters in the **CSAV On-access Task Statistics** dialog box cannot be reset. The statistics shown increase as files are scanned and infected files are found. For example, if the number of **Infected** files is **15** and you click **Reset Statistics**, the numeral is reset to **0**, but if 15 more infected files are found, the **Infected** count is **30**.

The **CSAV On-access Task Statistics** dialog box also contains two buttons not found in the **CSAV On-demand Task Statistics** dialog box. These two buttons are **Enable/Disable** and **Refresh**. **Enable/Disable** starts or stops the on-access scan task and **Refresh** provides up-to-the-moment on-access scan information.

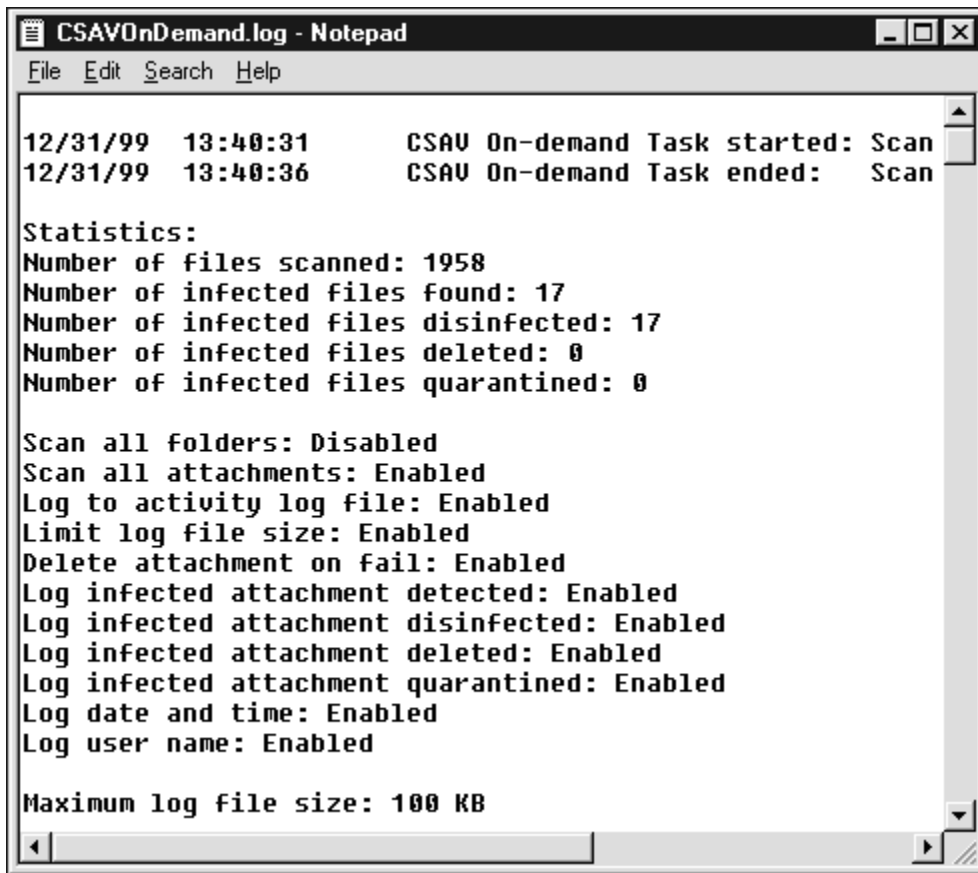
You can save the information in the **Statistics** dialog box to a text file by clicking the **Create Report** button. The system displays the **Save As** dialog box. Name the file and save it.

VIEWING THE LOG FILES

The **View Log** menu item allows you to view the contents of the on-demand or on-access log file. The on-demand log file contains information on how many infected files were found, disinfected, quarantined, or deleted. The on-access log file contains the name of the infected file, the type of virus that infected the message, the CSAV status of the message, and the date and time of the scan.

To view the log file for the on-access scan task or an on-demand scan task, follow these steps:

1. In the **Task List**, select a scan task name.
2. On the menu bar, click **Task**. The system displays the **Task** menu.
3. Click **View Log**. The system displays the log file:



```
CSAVOnDemand.log - Notepad
File Edit Search Help
12/31/99 13:40:31 CSAV On-demand Task started: Scan
12/31/99 13:40:36 CSAV On-demand Task ended: Scan

Statistics:
Number of files scanned: 1958
Number of infected files found: 17
Number of infected files disinfected: 17
Number of infected files deleted: 0
Number of infected files quarantined: 0

Scan all folders: Disabled
Scan all attachments: Enabled
Log to activity log file: Enabled
Limit log file size: Enabled
Delete attachment on fail: Enabled
Log infected attachment detected: Enabled
Log infected attachment disinfected: Enabled
Log infected attachment deleted: Enabled
Log infected attachment quarantined: Enabled
Log date and time: Enabled
Log user name: Enabled

Maximum log file size: 100 KB
```

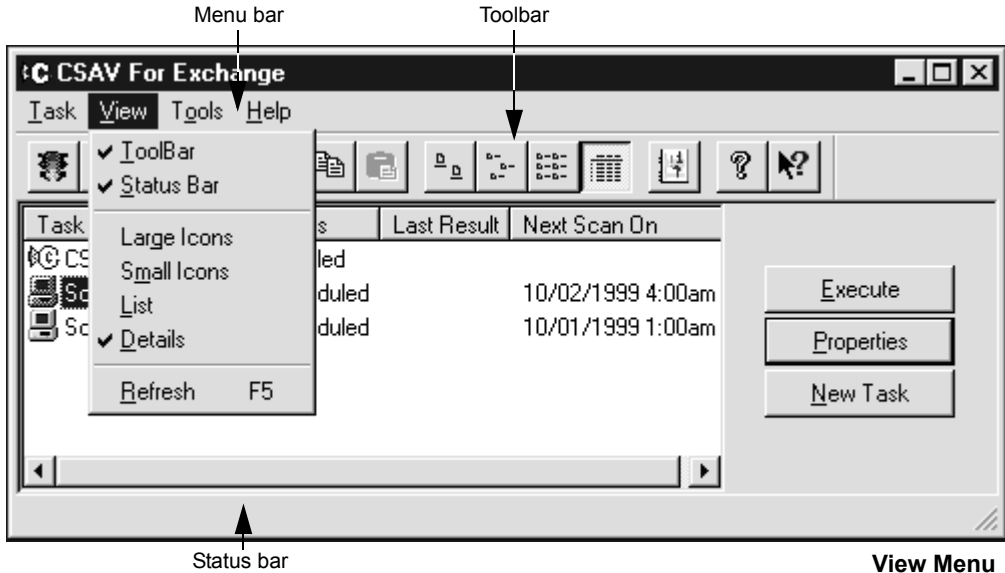
CSAV On-demand Log File



NOTE: If you have created a separate log file for a scan task, that log file displays when you click **View Log**. For more information, refer to [Reports located on page 3-40](#) in **Configuring Scanning Properties**.

USING THE VIEW MENU

The **View** menu allows you to change the appearance of the **Task List** as well as turn the **Toolbar** and **Status** bar on or off. The **View** menu also allows you to get the latest scan results by using the **Refresh** menu item.



TOOLBAR

This menu item turns the toolbar on or off. From the **Toolbar** you can create, modify, delete, and run scan tasks. The toolbar also contains buttons for getting product help and changing the appearance of the **Task List**.



NOTE: You can move the mouse pointer over any toolbar button to display a ToolTip that identifies the function of that particular button.

STATUS BAR

This menu item turns the status bar on or off. The status bar displays the current state of a scan action. For example, if you start an on-demand scan, the status bar displays the following message: “Executing the On-demand Scanning”.

LARGE ICONS

This menu item displays the **Task List** as scan task names appearing below large icons.

SMALL ICONS

This menu item displays the **Task List** as scan task names located to the right of small icons.

LIST

This menu item displays the **Task List** as a column of scan task names located to the right of small icons.

DETAILS

As with the **List** item, **Details** displays the **Task List** as a column of scan task names located to the right of small icons. Four column headers, **Task Name**, **Status**, **Last Results**, and **Next Scan On** also display.

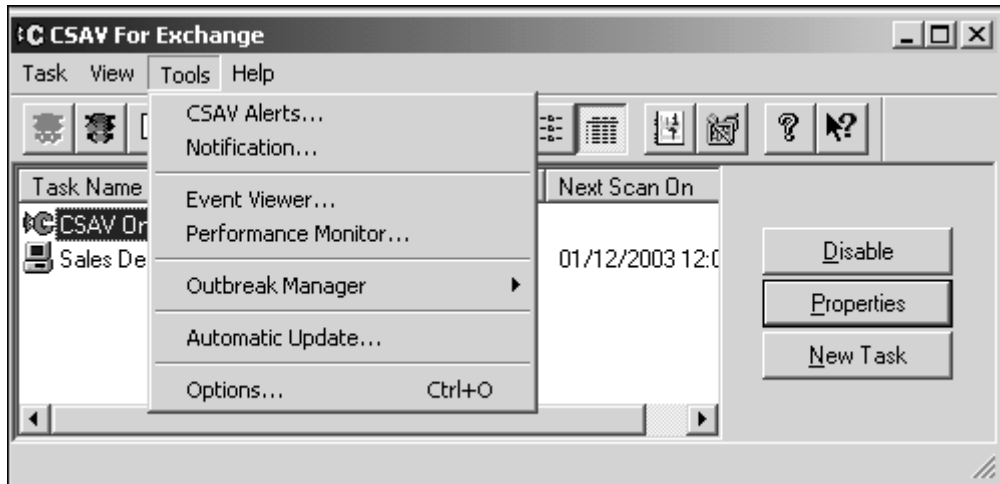
REFRESH

This item updates the status of scan tasks in the **Task Window**. For the on-access scan task, the status is updated to either **Disabled** or **Enabled**. For an on-demand scan task, the **Status**, **Last Results**, and **Next Scan On** date are updated.

USING THE TOOLS MENU

The **Tools** menu consists of the following items: **CSAV Alerts**, **Notification**, **Event Viewer**, **Performance Monitor**, **Outbreak Manager**, **Automatic Update**, and **Options**.

- **CSAV Alerts** – Allows you to send trap notifications to other computers using Simple Network Management Protocol (SNMP) when traps are generated by CSAV.
- **Notification** – Allows you to send virus-related messages to additional administrators when CSAV detects a virus-infected attachment through the on-access scan task.
- **Event Viewer** – Allows you to view monitoring and troubleshooting messages from CSAV from within Windows Event Viewer.
- **Performance Monitor** – Allows you to view the utilization of CSAV from within the Windows Performance Monitor.
- **Outbreak Manager** – Allows you to define and configure rules to manage infected items received by the Exchange Server.
- **Automatic Update** – Allows CSAV to update itself automatically with the latest program files and virus definitions. For more information, refer to the [Automatic Update](#) chapter.
- **Options** – Allows you to change the name of the Exchange Server administrator that was specified during installation. This mailbox is used to send SMTP alert messages when a virus-infected attachment is detected through the on-access scan task. You can also set the quarantine folder that temporarily holds infected e-mail objects.



Tools Menu

CSAV ALERTS

When CSAV for Exchange generates traps, you can send notifications to other computers using Simple Network Management Protocol (SNMP).

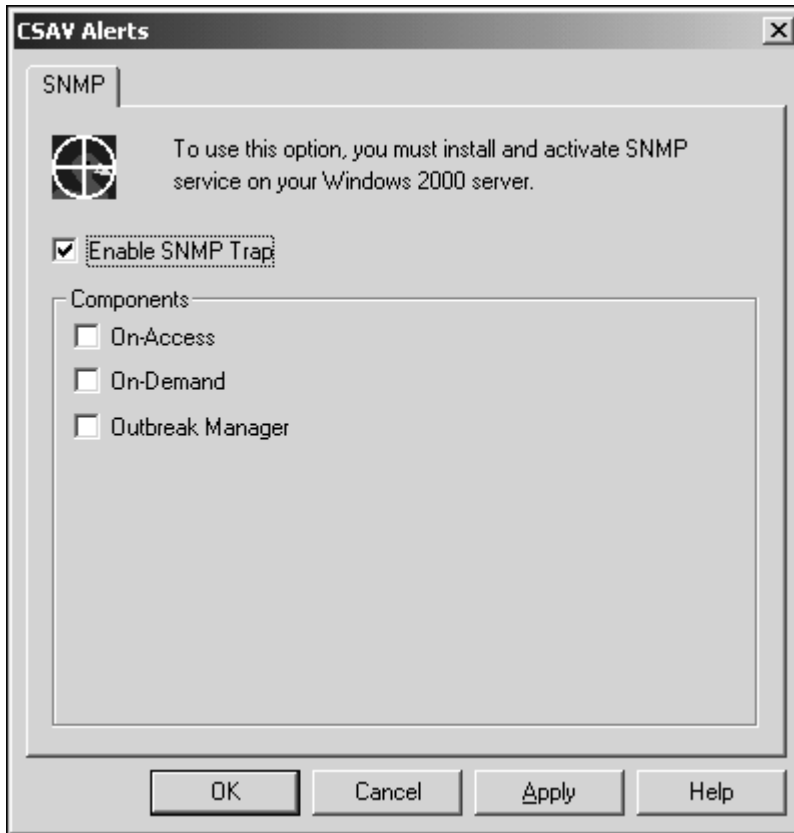


NOTE: SNMP **must** be installed and enabled on your Windows 2000 Server before trap notifications can be sent.

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

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

1. On the menu bar, click **Tools**. The system displays the **Tools** menu.
2. Click **CSAV Alerts**. The system displays the **CSAV Alerts** dialog box:



CSAV Alerts Dialog Box

3. Select the **Enable SNMP Trap** check box.
4. Under **components**, select one or more of the following:
 - On-Access – Allows CSAV for Exchange to send trap notifications when on-access scans are performed.
 - On-Demand – Allows CSAV for Exchange to send trap notifications when on-demand scans are performed.

- Outbreak Manager – Allows CSAV for Exchange to send trap notifications when an outbreak condition occurs. For more information about outbreak conditions, refer to [Outbreak Manager located on page 3-66](#).

5. Click **OK**.

VIRUS NOTIFICATION

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



NOTE: You can cancel sending a **mail alert message** to the Microsoft Exchange Server Administrator during the installation by clearing the **Send alerts to administrator** check box in the **CSAV for Exchange Options** dialog box. You can also cancel this **mail alert message** from the **CSAV for Exchange Console** menu bar by clicking **Tools**, and then clicking **Options**. For more information refer to [Options located on page 3-79](#).

You can send a **mail alert message** to additional administrators, and you can change the text of the messages that are sent.



NOTE: This option does **not** change the Microsoft Exchange Server Administrator that you specified during the installation. To change the Microsoft Exchange Server Administrator, on the **CSAV for Exchange Console** menu bar, click **Tools**, and then click **Options**. For more information, refer to [Options located on page 3-79](#).

Command AntiVirus for Exchange sends notifications only after an infected e-mail attachment has been:

- Sent and then saved in the **Sent Items** folder
- Received in the **Inbox** or in a **Public Folder**

Notifications are **not** sent if a virus is detected through an on-demand scan. However, if you have selected **Send the mail alert to Recipient(s)** for the on-access scan task, CSAV appends a **Scanning Summary** to the body of the e-mail that contained the infected attachment. The e-mail is then sent to its intended recipients.



NOTE: CSAV sends a single **mail alert message** for e-mail containing multiple infected attachments. For example, if CSAV detects an e-mail containing six infected attachments, one **mail alert message** containing notification of the six infected attachments is sent to the sender, the intended recipients, the Microsoft Exchange Server Administrator and any other additional administrators that have been specified.

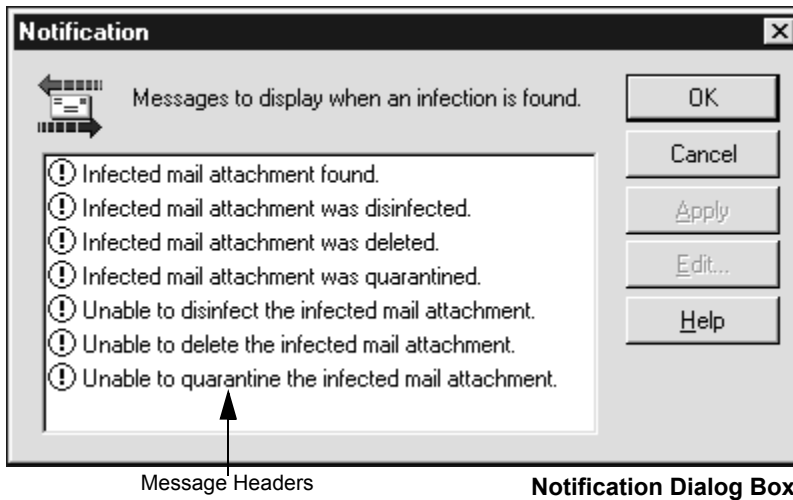
Customizing Virus Notifications

Customizing virus notifications consists of:

- Selecting a message header.
- Specifying who receives **mail alert messages** when a virus is detected through an on-access scan. This can include the sender of an infected e-mail, the e-mail's intended recipients, and selected administrators.
- Modifying the **mail alert messages** associated with the message header.

To customize virus notifications, follow these steps:

1. In the **Task List**, select the on-access scan task.
2. On the menu bar, click **Tools**. The system displays the **Tools** menu.
3. Click **Notification**. The system displays the **Notification** dialog box:

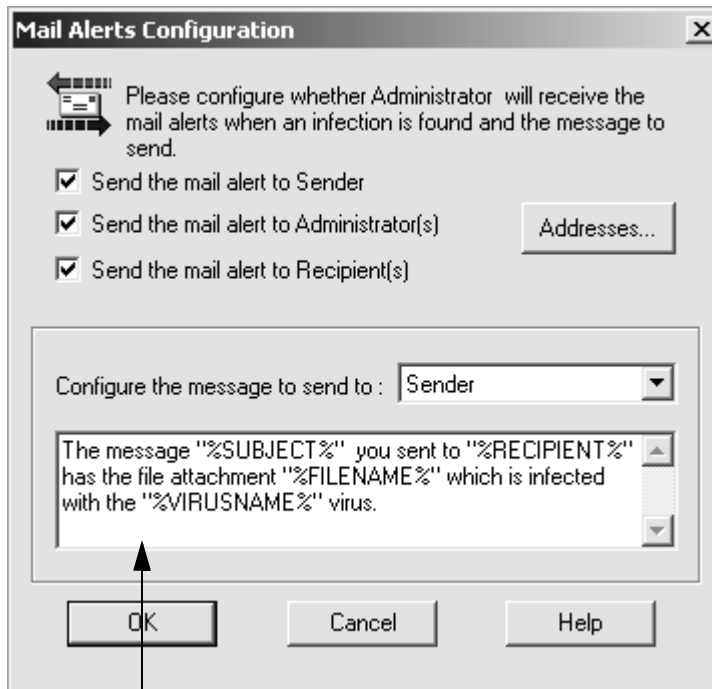


4. Select a message header, for example, **Infected Mail Attachment Found**.



NOTE: All message headers are enabled by default. They cannot be deleted or edited. Only the **mail alert messages** that are associated with each header can be edited.

5. Click **Edit**. The system displays the **Mail Alerts Configuration** dialog box:



Mail Alert Message Text Box **Mail Alerts Configuration Dialog Box**

6. Select one or more of the following options. All are selected by default. Click an option to clear it.



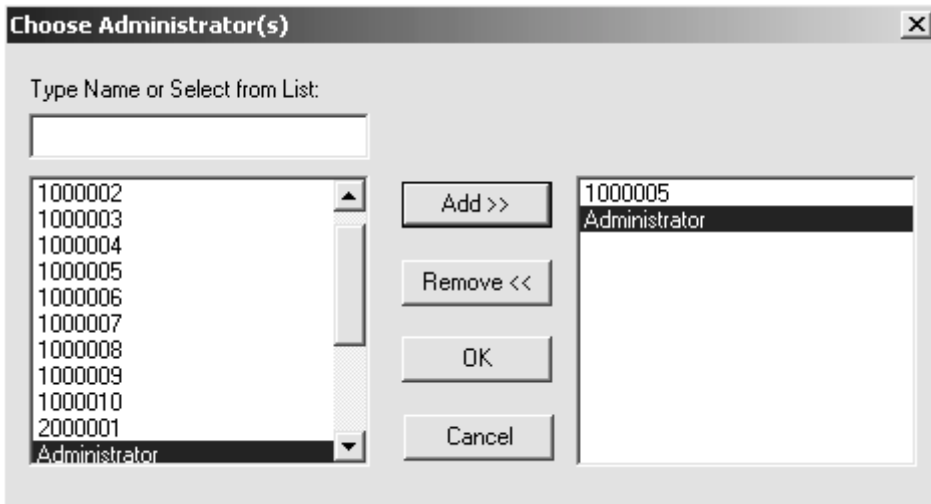
NOTE: If you clear **all** of these options, their message header in the **Notification** dialog box displays an **X** over its icon.

- Send the mail alert to Sender
- Send the mail alert to the Administrator(s)
- Send the mail alert to the Recipient(s)

If you select **Send the mail alert to Administrator(s)**, the **Addresses** button becomes available. Click the **Addresses** button to view the **Choose Administrator(s)** dialog box.



NOTE: This option does not change the Microsoft Exchange Server Administrator that you specified during the installation. To change the Microsoft Exchange Server Administrator, on the **CSAV for Exchange Console** menu bar, click **Tools**, and then click **Options**. For more information, refer to [Options located on page 3-79](#).



Choose Administrator(s) Dialog Box

From the list on the left, select the names of the people that you want to receive a mail alert message.



NOTE: To select multiple names, click the name, hold down the **Ctrl** key, and then click each additional name that you want to select.

To select a block of names, click the first name in the block, hold down the **Shift** key, and then click the last name in the block.



The **Choose Administrator(s)** dialog box can contain the names of persons who are **not** administrators. Use caution when selecting names from this dialog box.

After you make your selections, click **Add**. The system adds your selections to the list on the right.



NOTE: To remove a folder or recipient from the **right** window, select the folder or recipient, and click **Remove**.

Click **OK** to save your selections. The system returns to the **Mail Alerts Configuration** dialog box.

7. To modify the default **mail alert message**, click the **Configure the message to send to** drop-down arrow and select, for example, the **Sender**. The **mail alert message** that is sent to the **Sender** displays in the message text box.
8. Accept the default **mail alert message** for the **Sender** or edit it to fit your requirements.




NOTE: When editing a **mail alert message**, you can use variables that identify important aspects of the infected e-mail. For example, the “%VIRUSNAME%” variable can be used to identify the name of the virus that infected the e-mail’s attachment. For more information, refer to [Mail Alert Variables located on page A-2](#) in the **Appendix**.

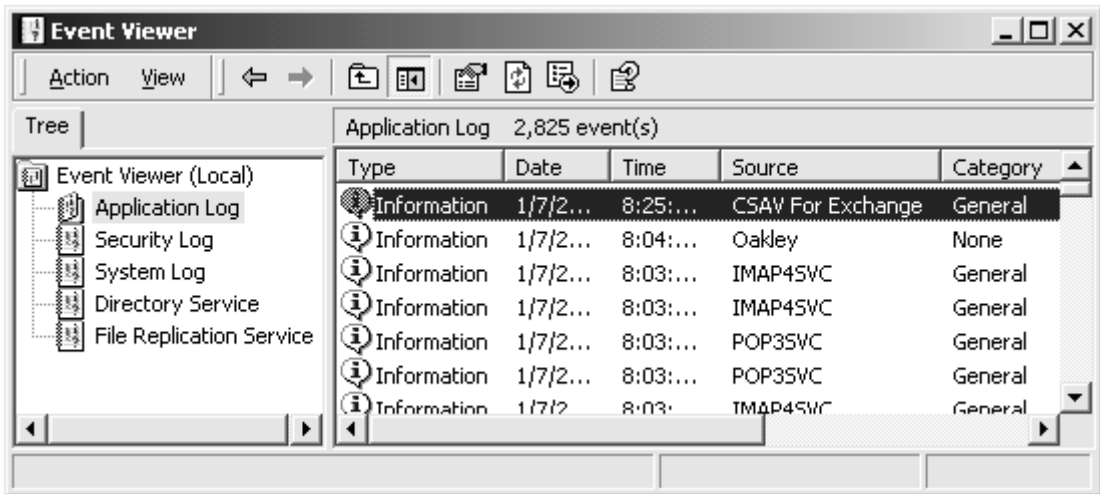
9. You can then reselect the **Configure message to send to** drop-down arrow and repeat **Step 6** and **Step 7** for **Recipient(s)** and the **Administrator(s)**.
10. Click **OK** to save your changes, and return to the **Notification** dialog box.

You can always return to the **Mail Alerts Configuration** dialog box to modify the **mail alert messages**.

USING EVENT VIEWER

In Windows **Event Viewer**, you can view which CSAV events started or ended. You can also view basic scan task statistics such as the number of files scanned, infected, disinfected, deleted, and moved.

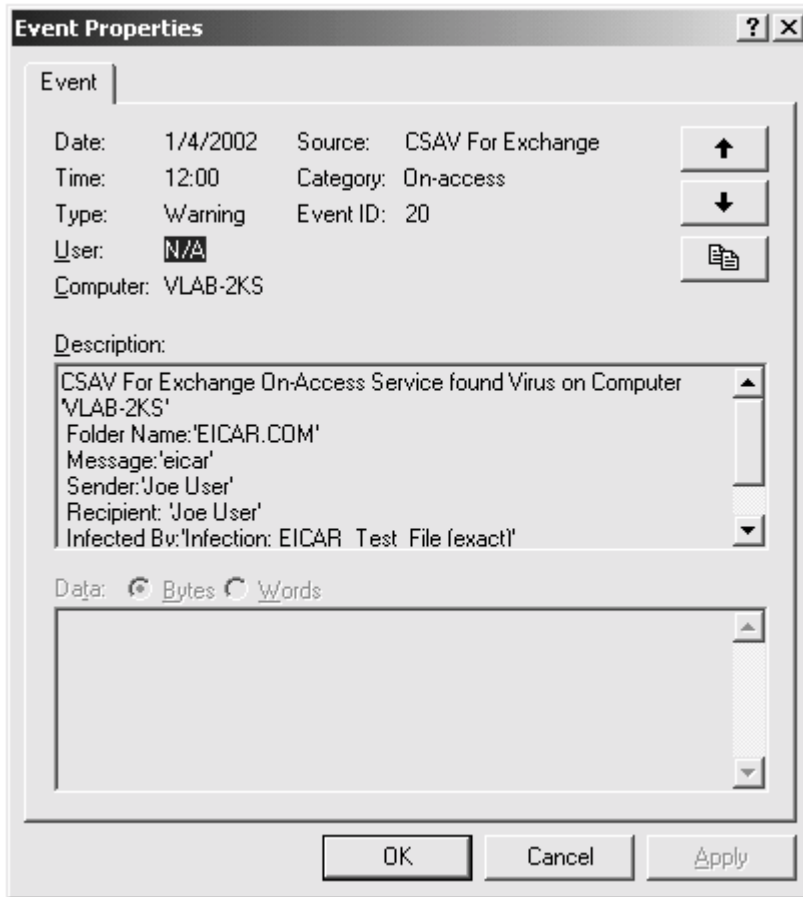
To access **Event Viewer**, you can click the **Event Viewer** button  on the CSAV for Exchange toolbar. The system displays the **Event Viewer**. In **Event Viewer Tree**, select **Application Log**. The system displays the log of events in the right pane:



Windows Event Viewer

CSAV for Exchange uses four categories to identify events: **General**, **On-demand**, **On-access**, and **Scheduler**. These categories can be found in the **Category** column.

Each CSAV for Exchange category contains several application-related events. To see a detailed description of any CSAV event found in the **Category** column, double-click the row pertaining to the event. The system displays an **Event Properties** dialog box with information on the event:



Event Properties Dialog Box

OUTBREAK MANAGER

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

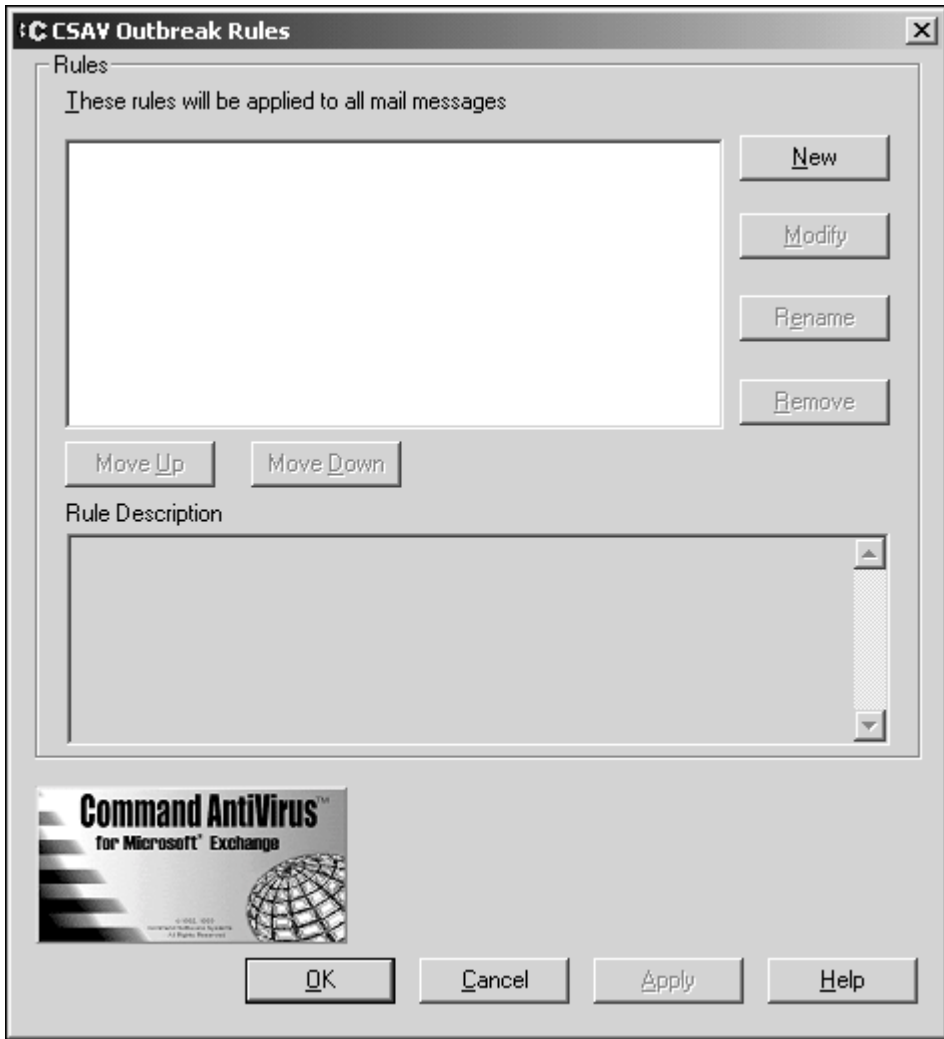
- **Configure Rules** specific to your environment.
- Define **Outbreak Conditions** for each configured rule.
- Define the **Outbreak Actions** to be taken for each defined condition.
- Set up a log file using **Log File Settings**. You can specify the file path and file size.
- View the log file that you set up using **View log**.
- **Show Tray Icon** in the notification area to the right of the taskbar.



NOTE: You cannot configure more than 5 rules.

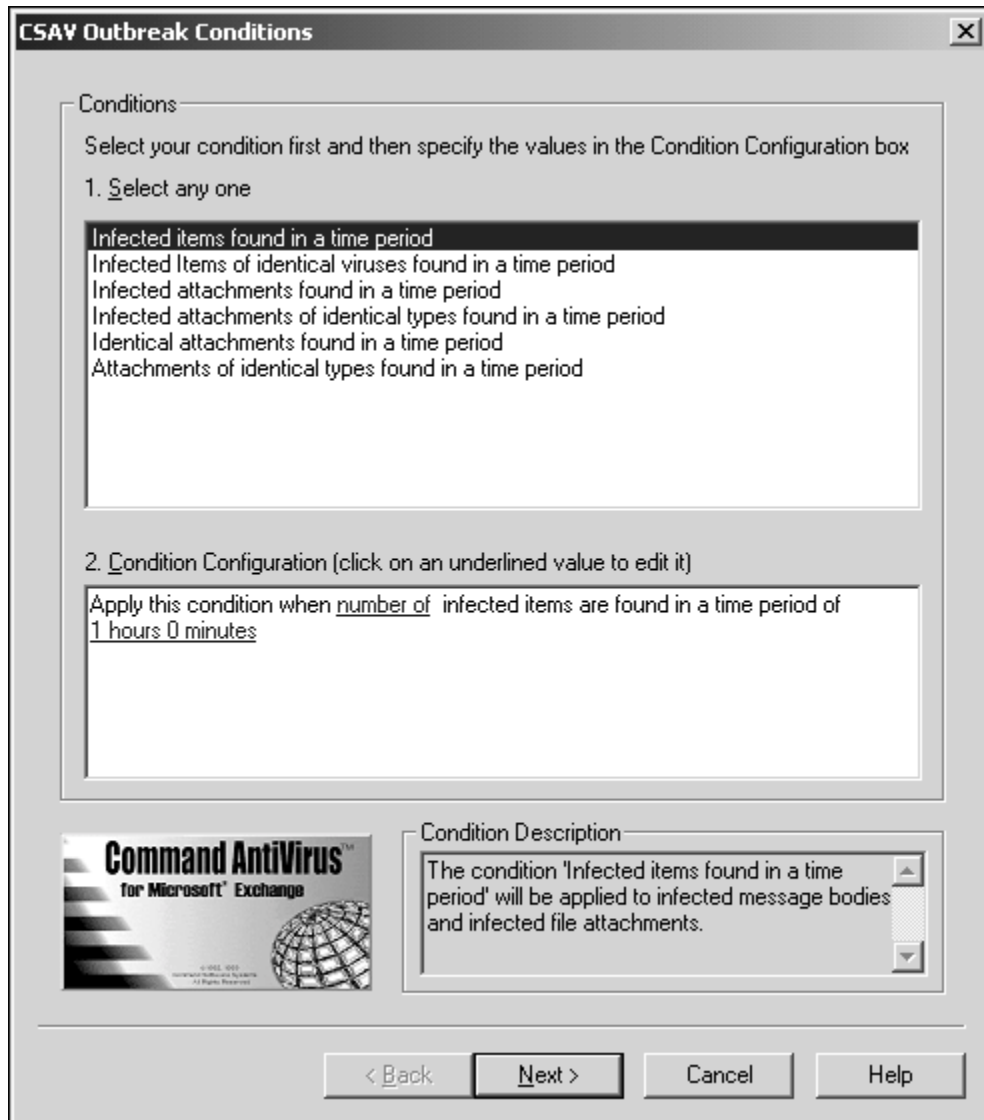
To set up **Configuration Rules**, **Outbreak Conditions**, and **Outbreak Actions**, follow these steps:

1. On the menu bar, click **Tools**. The system displays the **Tools** menu.
2. Click **Outbreak Manager**, and then click **Configure0 Rules**. The system displays the **CSAV Outbreak Rules** dialog box:



CSAV Outbreak Rules Dialog Box

3. Click **New**. The system displays the **CSAV Outbreak Conditions** dialog box:

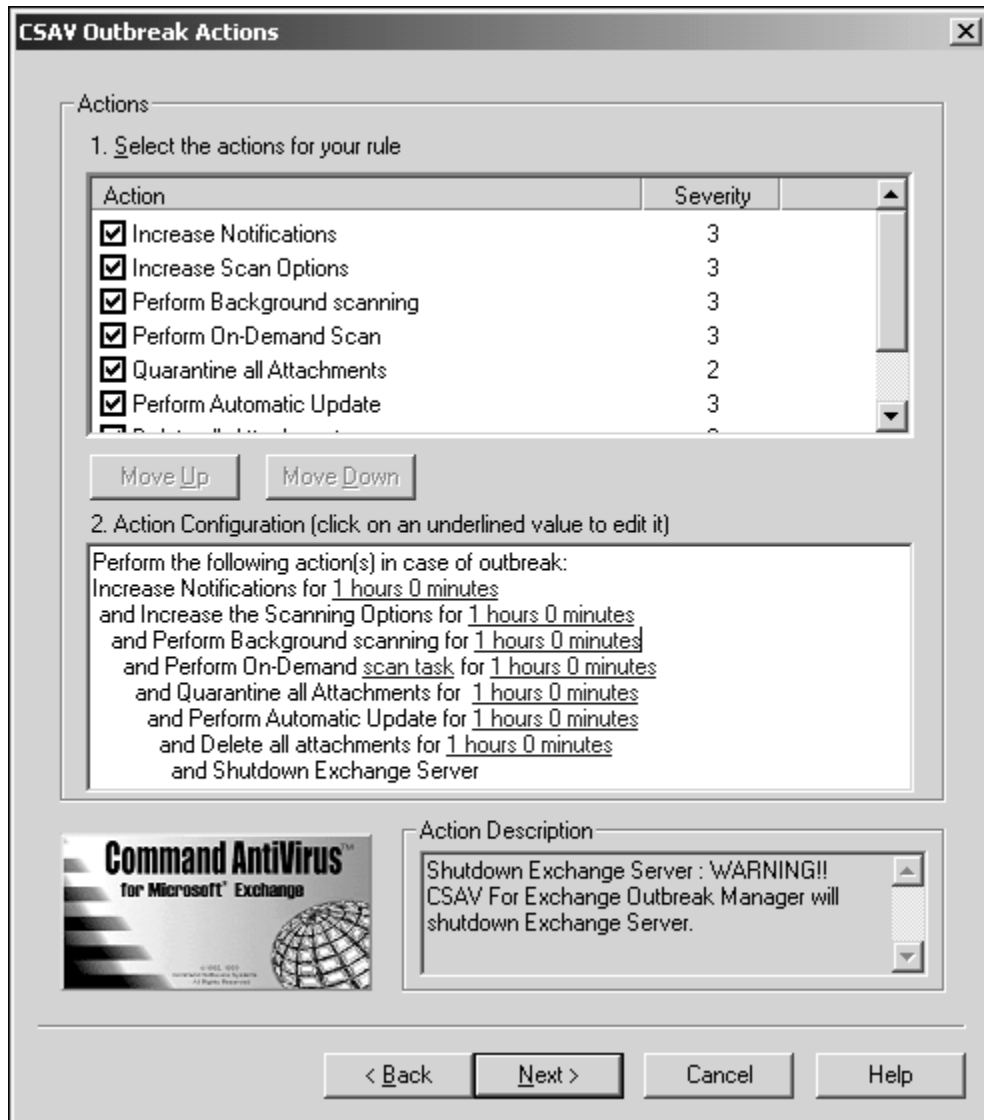


CSAV Outbreak Conditions Dialog Box

4. In the **Conditions** list box, select one of the following conditions:
 - Infected items found in a time period
 - Infected items of identical viruses found in a time period
 - Infected attachments found in a time period
 - Infected attachments of identical types found in a time period
 - Identical attachments found in a time period
 - Attachments of identical types found in a time period

When you select a condition, a description of the condition displays in the **Condition Description** window at the bottom of the dialog box.

5. In the Condition Configuration box, click the **number of** and **1 hours 0 minutes** values to specify the number of items to be found in a period of time for the condition to be applied.
6. Click **Next**. The system displays the **CSAV Outbreak Actions** dialog box displays:



CSAV Outbreak Actions Dialog Box

7. Under **Actions**, select one or more of the following actions to be taken when the defined condition is met:
 - Increase Scan Options
 - Increase Notifications
 - Perform Automatic Update
 - Perform On-Demand Scan
 - Perform Background scanning
 - Quarantine all Attachments
 - Delete all Attachments
 - Shutdown Exchange Server

When you select a condition, a description of the condition displays in the **Condition Description** window at the bottom of the dialog box.

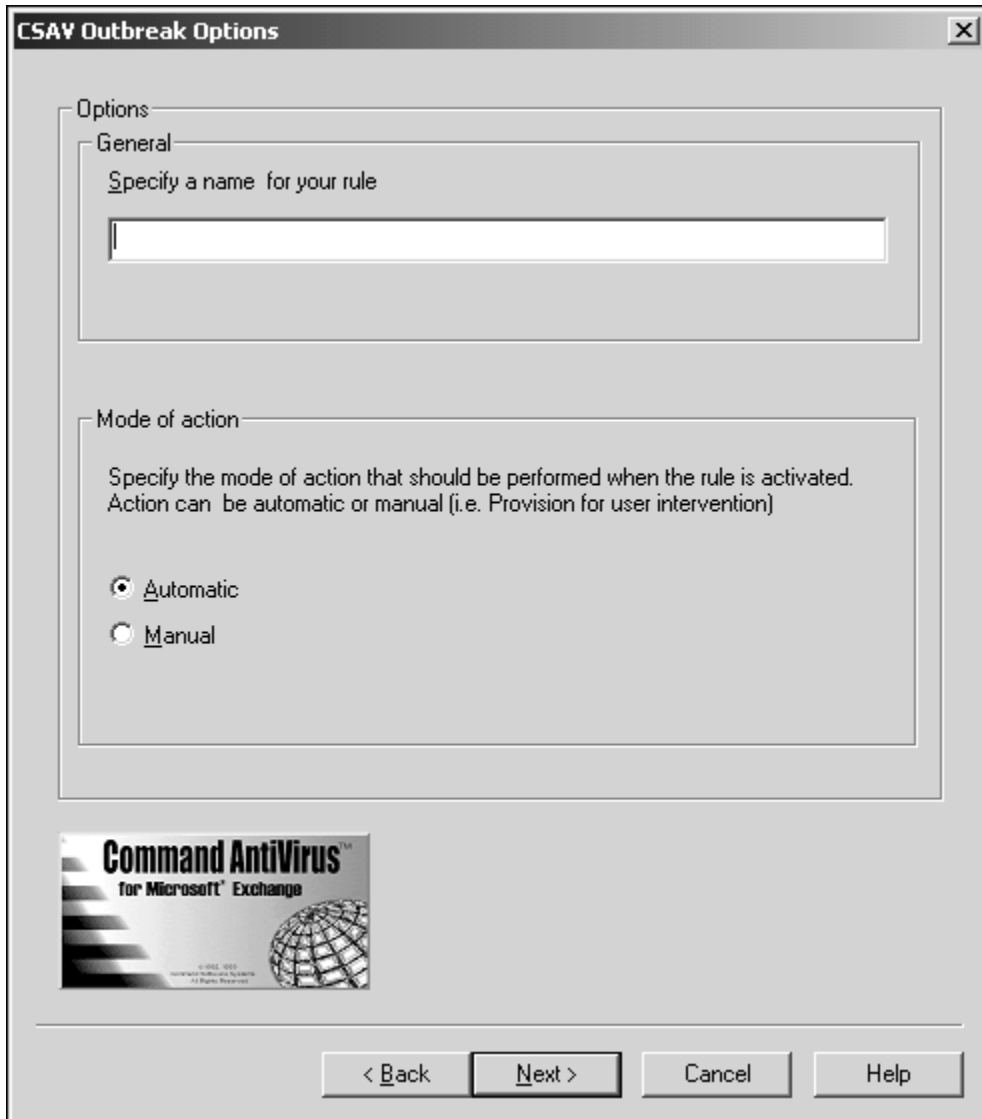
8. Click the **Move Up** and **Move Down** buttons to set the execution order of the rules you have selected.
9. In the **Action Configuration** box, define the values associated with the action selected under Actions. Values needing to be defined are in blue text and are underlined. Values needing to be defined include the name of the on-demand scan (scan task) and the time period (1hours 0minutes). Click each value and enter the required information in the corresponding dialog box.



NOTE: You do not need to specify all values for each condition.

When you select an action, a description of the action displays in the **Action Description** window at the bottom of the dialog box.

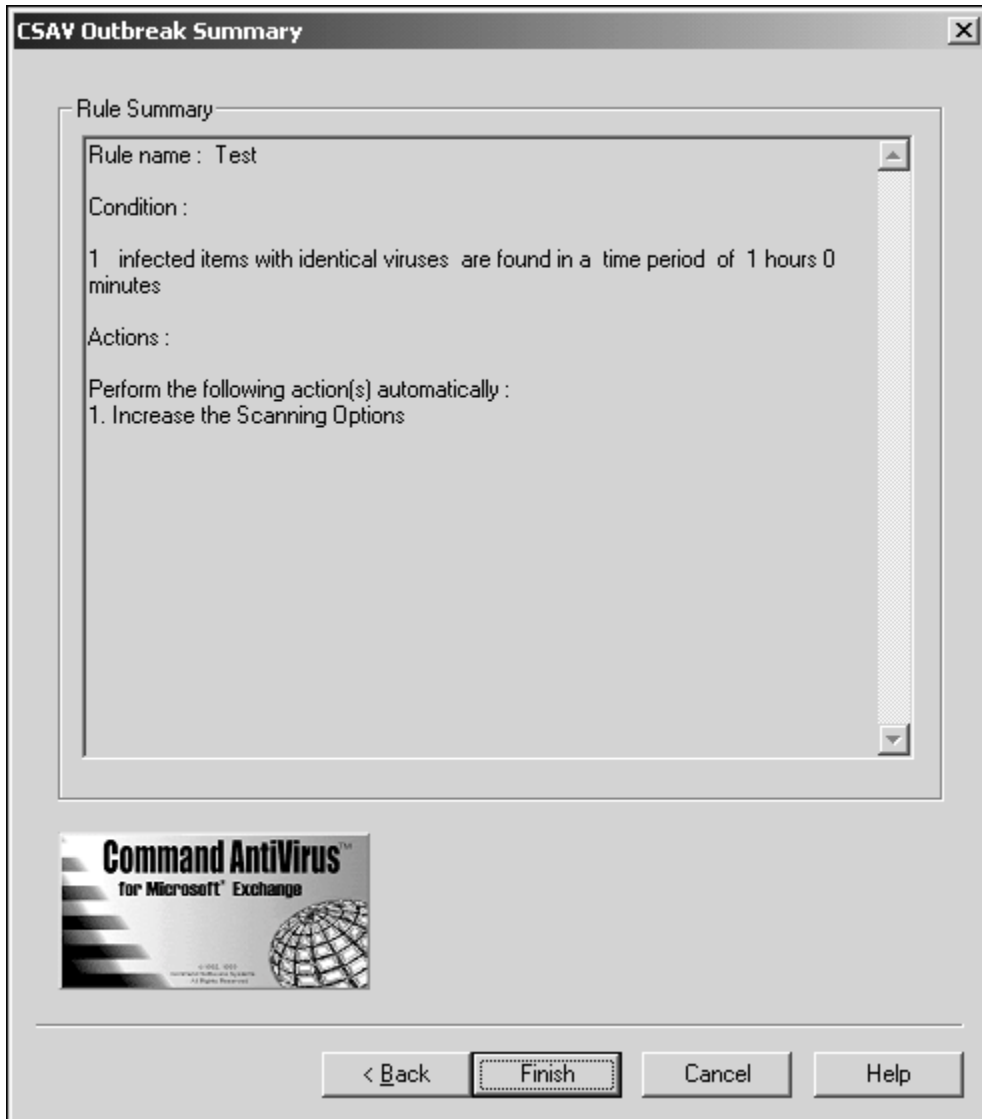
10. Click **Next**. The system displays the **CSAV Outbreak Options** dialog box:



CSAV Outbreak Options Dialog Box

11. In the **General** text box, type the name of the configuration rule.

12. Under **Mode of action**, select one of the following:
 - **Automatic** – Automatically activates the configuration rule
 - **Manual** – Allows you to manually activate the configuration rule
13. Click **Next**. The system displays the **CSAV Outbreak Summary** dialog box:



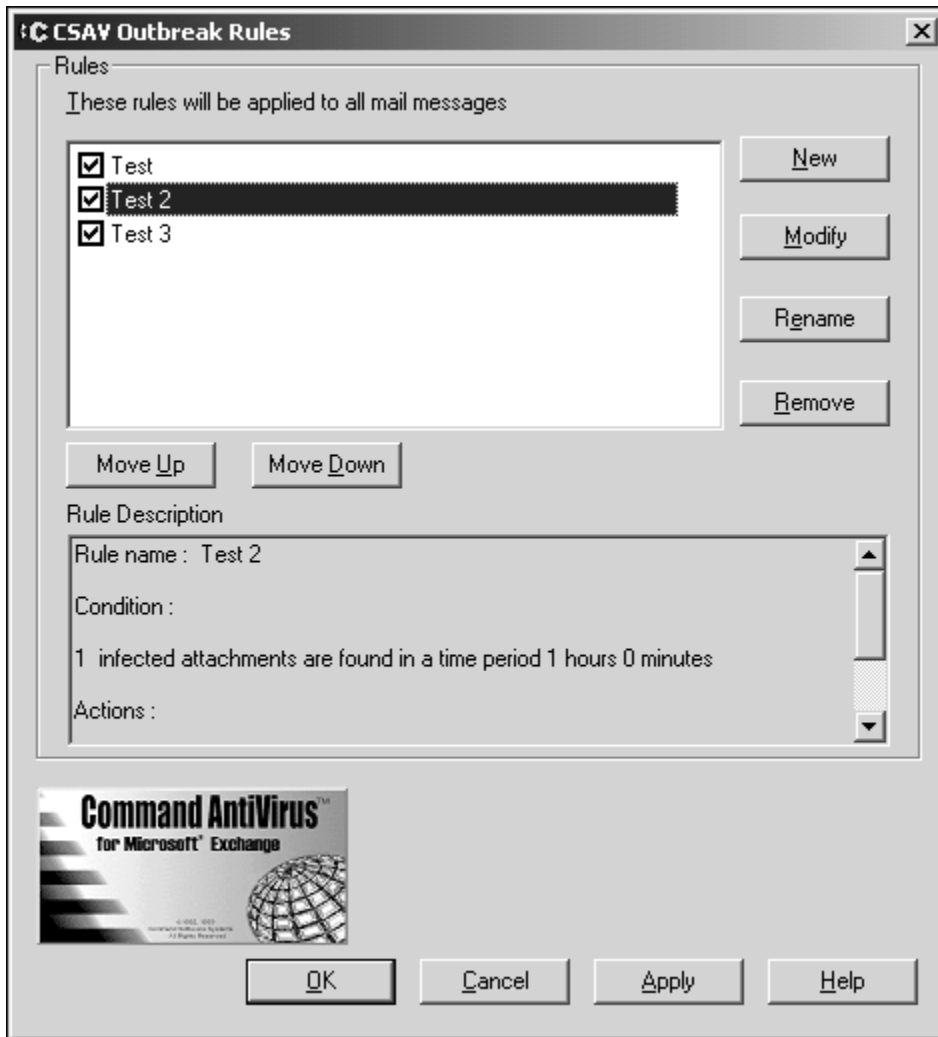
CSAV Outbreak Summary Dialog Box

14. Review the summary of the configured rule, and click **Finish**.



NOTE: If you want to change any information, click **Back** to the appropriate dialog box.

The **CSAV Outbreak Rules** dialog box displays with the new configuration rules listed:



CSAV Outbreak Rules Dialog Box

15. Click the **Move Up** and **Move Down** buttons to set the execution order of the rules you have selected.

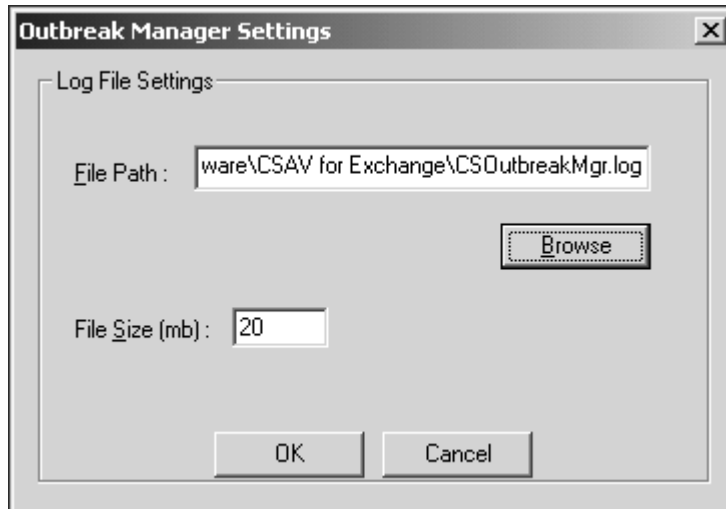
16. Click **Apply**, and then click **OK**.



NOTE: You can modify, rename, or remove any **Configuration Rule** in the **CSAV Outbreak Rules** dialog box.

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

1. On the menu bar, click **Tools**. The system displays the **Tools** menu.
2. Click **Outbreak Manager**, and then click **Log File Settings**. The system displays the **Outbreak Manager Settings** dialog box:

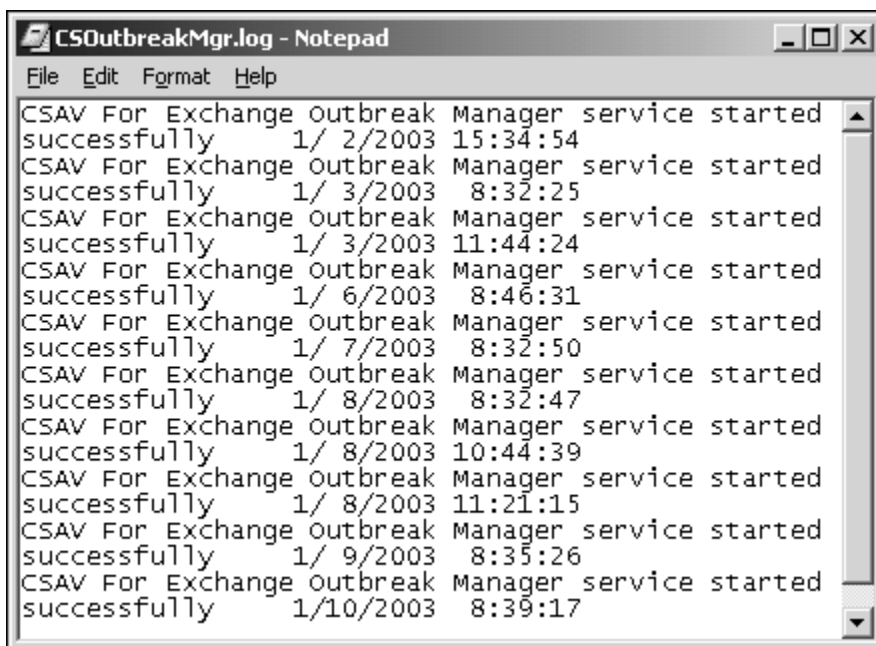


Outbreak Manager Settings Dialog Box

3. By default, the log file is placed in `C:\Program Files\Command Software\CSAV For Exchange\CSOutbreakMgr.log`. If you want to place your log file in a different location, click **Browse** to find the correct location.
4. The default log file size is 20 MB. If you want a different size log file, enter the size in the **File Size** text box.

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

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



```
CSAV For Exchange Outbreak Manager service started
successfully 1/ 2/2003 15:34:54
CSAV For Exchange Outbreak Manager service started
successfully 1/ 3/2003 8:32:25
CSAV For Exchange Outbreak Manager service started
successfully 1/ 3/2003 11:44:24
CSAV For Exchange Outbreak Manager service started
successfully 1/ 6/2003 8:46:31
CSAV For Exchange Outbreak Manager service started
successfully 1/ 7/2003 8:32:50
CSAV For Exchange Outbreak Manager service started
successfully 1/ 8/2003 8:32:47
CSAV For Exchange Outbreak Manager service started
successfully 1/ 8/2003 10:44:39
CSAV For Exchange Outbreak Manager service started
successfully 1/ 8/2003 11:21:15
CSAV For Exchange Outbreak Manager service started
successfully 1/ 9/2003 8:35:26
CSAV For Exchange Outbreak Manager service started
successfully 1/10/2003 8:39:17
```

Outbreak Manager Log

OPTIONS

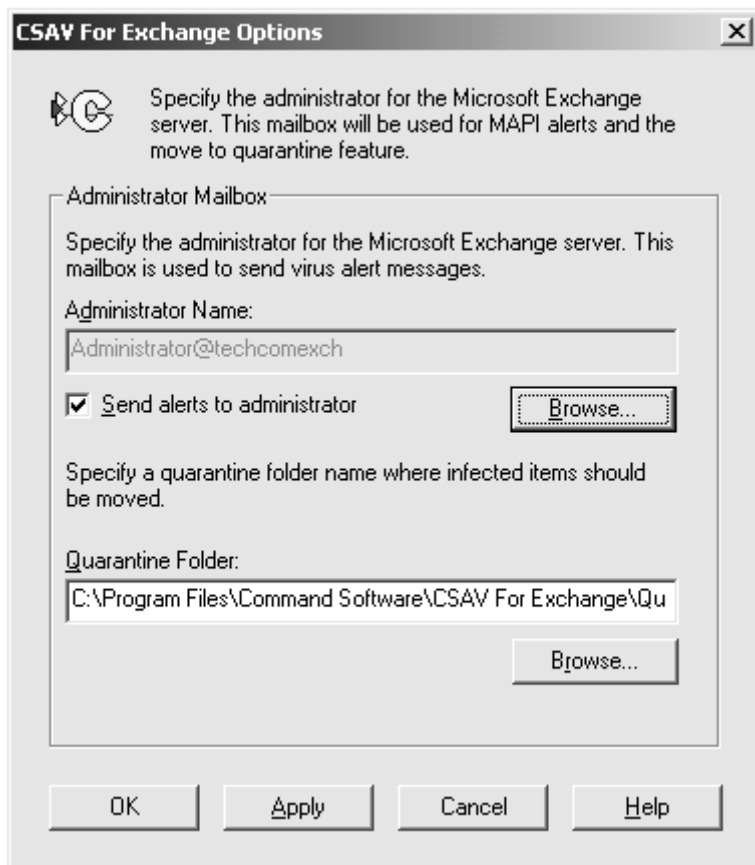
The **CSAV for Exchange Options** allows you to change the name of the Exchange Server administrator that was specified during installation. This mailbox is used to send SMTP alert messages when a virus-infected attachment is detected through the on-access scan task. You can also select **not** to send an alert message to the Exchange Server administrator, and you can set the quarantine folder that temporarily holds infected e-mail objects.



NOTE: You can configure CSAV for Exchange to send virus notifications to more than one administrator. For more information, refer to [Customizing Virus Notifications](#) located on page 3-59.

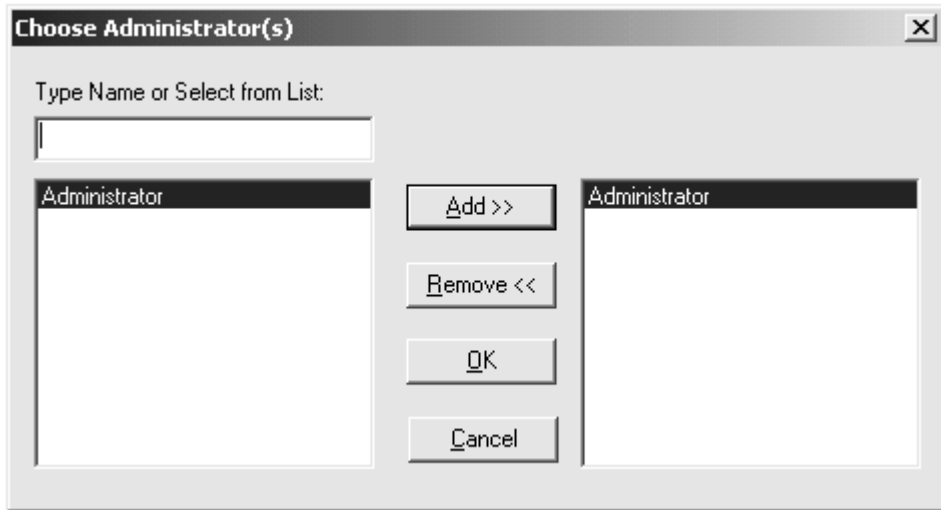
To set the **Administrator Name** and the **Quarantine Folder**, follow these steps:

1. On the menu bar, click **Tools**. The system displays the **Tools** menu.
2. Click **Options**. The system displays the **CSAV for Exchange Options** dialog box:



CSAV For Exchange Options Dialog Box

3. In the **Administrator Mailbox** group box, click the **Browse** button. The system displays the **Choose Administrator(s)** dialog box:



Choose Administrator(s) Dialog Box

4. Select an administrator from the list of available names and click **Add**.



NOTE: This selection changes the name of the Exchange Server Administrator that was specified during installation.



NOTE: To remove an administrator from the **right** window, select the administrator and click **Remove**.

5. Click **OK**. The system returns to the **CSAV for Exchange Options** dialog box.



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

- In the **Quarantine Folder** text box, specify the path to the quarantine folder. The default is `Program Files\Command Software\CSAV for Exchange\Quarantine`. To change the path, click the **Browse** button. The system displays the **Browse for Folder** dialog box:



Browse for Folder Dialog Box

- Select a quarantine folder from the list of available folders.
- Click **OK**. The system redisplay the **CSAV for Exchange Options** dialog box.

HELP MENU

The **Help** menu items allow you to locate information on topics of interest including instruction on how to use the features found in CSAV for Exchange. You can access this menu by clicking **Help** on the menu bar.

INDEX

Displays the **Help Topics** dialog box with **Contents**, **Index** and **Find** tabs. The **Contents** tab lists major topics. The **Index** tab provides an alphabetical listing of all topics. The **Find** tab allows you to search for a topic by key word. You can select topics from the contents or the index for easy access to information.

USING HELP

This menu item displays a list of topics on the **Help** menu items. Click a topic to view detailed information on the topic.

TECHNICAL SUPPORT

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

ERROR REPORT

This menu allows you to report any problems you may be experiencing with CSAV for Exchange. Make sure you provide all the requested information, and as much detailed information as you can, so that the technical support representative can help you solve your problem as quickly as possible.

ABOUT CSAV FOR EXCHANGE

This menu item displays the product's version number, copyright information, scan engine information, and system information.

CONFIGURING THE MESSAGE.INI FILE

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

By default, the file name of the new attachment contains the original file name and with the extension **.VIRUS INFO.TXT** added to it.

For example, if the original file name and extension is **EICAR1.COM**, the name of the new attachment is:

```
EICAR1.COM.VIRUS INFO.TXT
```

You can customize the file name of the new attachment and the additional information message contained in it by editing the **MESSAGE.INI** file.

To edit the **MESSAGE.INI** file, follow these steps:

1. Locate the **MESSAGE.INI** file.
2. Using a text editor, open the file.
3. Locate the **FileName =** parameter. The default file name information is contained in quotation marks ("").
4. Change the file name information.



NOTE: Make sure that your new file name information is contained within the quotation marks ("").

5. Locate the **Footer =** parameter.
6. Change the default message.
7. Save and close the file.

4

AUTOMATIC UPDATE

This chapter contains instructions on how to use the **Automatic Update** feature. This feature provides the easiest and most efficient method available for keeping the latest version of Command AntiVirus (CSAV) for Exchange running on your system. Using the **Automatic Update** feature assures that your Exchange mail system is always being protected by the latest antivirus technology.

PREPARING FOR THE AUTOMATIC UPDATE



NOTE: To use the **Automatic Update** feature, Command AntiVirus must be installed on each Microsoft® Exchange server that will be updated.



NOTE: **Automatic Update** performs CSAV for Exchange component updates. To perform a full-product update, you must run SETUP **manually** from the CSAV for Exchange server.

CREATING THE AUTOMATIC UPDATE DIRECTORY

The **Automatic Update** feature operates by downloading update files into the Windows® temporary directory. This directory is called the **staging directory**. These files are then immediately decompressed into a unique parent directory in a shared location on the network. This directory is called the **automatic update directory**. CSAV for Exchange then uses the files that were decompressed into the **automatic update directory** to update itself.



NOTE: The server conducting the update must have **Read** access to the shared Universal Naming Convention (UNC) location that contains the **automatic update directory**.

Before CSAV can perform automatic updates, you must create the **automatic update directory**.

Create the **automatic update directory** on a shared location on the network, for example:

```
\\SERVER\SHARE\UPDATE
```

Then, when an on-demand or scheduled update takes place, CSAV for Exchange does the following:

1. Downloads the update files from the FTP site to the **staging directory**.
2. Creates a CSAV for Exchange product directory within the **automatic update directory**. The product directory is always a specific number, for example:

```
\\SERVER\SHARE\UPDATE\0604
```

3. Creates separate subdirectories for the virus definition files and the update component files. The definition files subdirectory ends in **.00**. The component files subdirectory ends in **.01**. The file names are generated randomly by CSAV for Exchange. The following is an example of the path names to the automatic update directory and its subdirectories:

```
\\SERVER\SHARE\UPDATE\0604
\\SERVER\SHARE\UPDATE\0604\CSS43e.00
\\SERVER\SHARE\UPDATE\0604\CSS282.01
```

4. Creates a file named CSSFILES.INI containing the following information:

```
[Win32-CSAV_Exchange]
BaseDir=\\SERVER\SHARE\UPDATE\0604
Deffiles=CSS43e.00
Compont=CSS282.01
```

Decompresses the contents of the update file (component files, virus definitions, etc.) into the appropriate directories in the **automatic update directory**.



NOTE: Every update creates a new definition and a new component files subdirectory in the **automatic update directory**. Therefore, we recommend that you periodically delete old subdirectories.

5. Performs an immediate update of CSAV for Exchange.

CONFIGURING THE AUTOMATIC UPDATE

The **Automatic Update** dialog box contains options that you can modify for the automatic update process. The **Automatic Update** dialog box consists of the **Update** dialog box and the **Schedule** dialog box.

The **Update** dialog box is divided into two sections. The upper section contains the **FTP Site** group box. The lower section contains text boxes for the **Automatic Update directory path** and the **Staging directory path**.

By default, the **FTP Site** group box contains the primary FTP site IP address and product directory. It is from this site that CSAV for Exchange downloads its update files. You can add a secondary FTP site IP address and product directory. You can change the primary FTP site IP address and product directory if necessary.



If you decide to use a non-default FTP site IP address, be sure to provide the correct path to the CSAV for Exchange product directory at this address.

To open the **Automatic Update** dialog box, follow these steps:

1. On the menu bar, click **Tools**. The system displays the **Tools** menu.
2. Click **Automatic Update**. The system displays the **Automatic Update** dialog box with the **Update** dialog box in view:

Automatic Update [X]

Update | Schedule

Use this page to specify where to obtain updates from.

FTP Site

Select FTP Site: Primary FTP site

Set the parameters for the Primary FTP site:

IP Address: ftp.commandsoftware.com

Product Directory: /products/commercial/CSSCntrl/

User Name:

Password:

Automatic Update directory path:
\\Automatic Update [Browse...]

Staging directory path:
C:\DOCUME~1\ADMINI~1\LOCALS~1\Ter [Browse...]

[Update now...]

[OK] [Cancel] [Apply] [Help]

Update Dialog Box

3. Under **FTP Site**, click the drop-down arrow in the **Select FTP Site** drop-down list box to select the **Primary FTP site** or the **Secondary FTP site**. For example, if you select the **Primary FTP site**, the information displayed in the **FTP Site** group box pertains only to the primary site.

The following information is required:

- **IP address** of the FTP site
- **Product Directory** on the FTP site
- **User Name** for the FTP site
- **Password** for the FTP site
- **Automatic Update directory path** of the **automatic update directory**
- **Staging directory path** of the **staging directory**

To complete the required information, follow these steps:

1. In the **Select FTP Site** drop-down list box, click the drop-down arrow.
2. From the drop-down list, select **Primary FTP site**.
3. If you want to download CSAV for Exchange updates from the default site, proceed to **Step 5**.

If you want to download from a different site, in the **IP Address** text box, type the IP address for the FTP site.

4. In the **Product Directory** text box, type the path to the CSAV for Exchange update directory located on the FTP site.
5. In the **User Name** text box, type your user name for the FTP site.
6. In the **Password** text box, type your password for the FTP site.
7. Repeat **Step 1** through **Step 6** for the **Secondary FTP site**.



NOTE: If the **Primary FTP site** is unavailable for downloads, CSAV for Exchange automatically tries to download from the **Secondary FTP site**. For this reason, we recommend that you always have complete and accurate secondary FTP information in the **FTP Site** group box.

8. In the **Automatic Update directory path** text box, type the path to the **automatic update directory**. You can also use the **Browse** button to locate this path.



NOTE: If you do not specify an **automatic update directory**, the automatic update process ends before the downloaded files are extracted.

9. In the **Staging directory path** text box, type the path to the **staging directory**. CSAV for Exchange uses the Windows temporary directory as the **staging directory**. You can use the **Browse** button to change this path.



NOTE: If you do not specify a **staging directory**, the download of the update files can not be performed.

10. Click **OK**.

PERFORMING AN AUTOMATIC UPDATE

You can perform an immediate update of CSAV for Exchange or you can schedule updates to take place at regular intervals.



NOTE: If the program determines that there are no CSAV for Exchange files that need to be updated, the automatic update process ends.

Update Now

After you have entered all of the necessary information in the **Update** dialog box, you can perform an on-demand update of CSAV for Exchange. To perform the update, click the **Update now** button. CSAV for Exchange downloads the latest update files and then immediately updates your system.

Scheduled Updates

You can configure CSAV for Exchange to download update files automatically according to a schedule that you set. The updating process occurs immediately upon the completion of the download.

To schedule downloads, follow these steps:

1. In the **Automatic Update** dialog box, click the **Schedule** tab. The system displays the **Schedule** dialog box:



NOTE: To access the **Schedule** dialog box, you **must** first provide your user name in the **Update** dialog box.

The screenshot shows the 'Automatic Update' dialog box with the 'Schedule' tab selected. The dialog box has a title bar with 'Automatic Update' and a close button. Below the title bar are two tabs: 'Update' and 'Schedule'. The 'Schedule' tab is active. The main area contains a clock icon and the text 'Schedule the execution of the automatic update.' Below this is a checked checkbox labeled 'Enable scheduling'. Underneath is a 'Scan frequency' section with three radio buttons: 'Daily', 'Weekly', and 'Monthly'. The 'Weekly' option is selected. To the right of 'Weekly' are checkboxes for days of the week: Mon, Tue, Wed, Thu, Fri, Sat, and Sun. The 'Sat' checkbox is checked. Below the 'Monthly' option is a dropdown menu showing '1st'. At the bottom of the main area is a field for 'Scheduled download time (12 hour format):' with '12:01' in a text box and 'AM' in a dropdown menu. Below this is the text 'Next Automatic Update scheduled on: 01/01/2000 12:01 am'. At the very bottom are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

Schedule Dialog Box

2. Select the **Enable Scheduling** check box.
3. Under **Scan frequency**, select **Daily**, **Monthly** or **Weekly**.
If you select **Weekly**, select the day(s) you want the scheduled downloads to occur.
If you select **Monthly**, click the down arrow to specify the day of the month you want the download to occur.
4. Using the **00:00** time format, in the **Scheduled download time (12 hour format)** text box, type the time you want the download to occur. Then, click the down arrow to select **AM** or **PM**.
5. Click **OK**.

Your CSAV for Exchange system is now configured to download update files according to the scheduling information you provided.



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.

APPENDIX

This appendix contains technical information on the special functions in Command AntiVirus™ for Microsoft® Exchange. Some of these functions allow you to accomplish tasks faster; others allow you to change the way the product works.

KEYBOARD SHORTCUTS

The keyboard shortcuts allow you to save time in navigating through the product. The following is a list of keyboard shortcuts for Command AntiVirus for Microsoft Exchange.

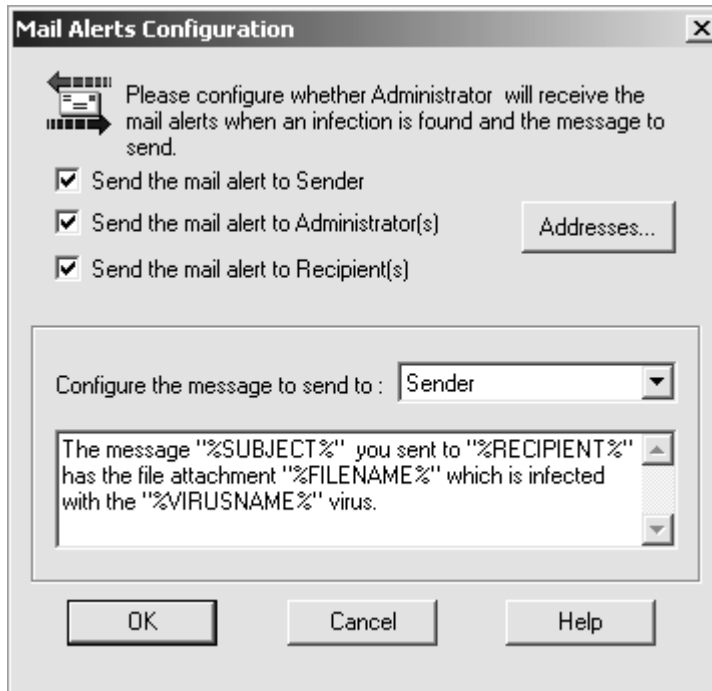
LIST OF KEYBOARD SHORTCUTS

Command	Keyboard Shortcuts
Task Menu	Alt + T
Task Menu – New Task	Alt + T and N
Task Menu – Disable	Alt + T and D
Task Menu – Rename Task	F2 or Alt + T and R
Task Menu – Delete Task	Alt + T and D
Task Menu – Properties	Ctrl + P
Task Menu – Cut	Ctrl + X
Task Menu – Copy	Ctrl + C
Task Menu – Paste	Ctrl + V
Task Menu – Statistics	Alt + T and S
Task Menu – View Log	Alt + T and V
Task Menu – Exit	Alt + T and X
View Menu	Alt + V
View Menu – Toolbar	Alt + V and T
View Menu – Status bar	Alt + V and S
View Menu – Large Icons	Alt + V and G

View Menu – Small Icons	Alt + V and M
View Menu – List	Alt + V and L
View Menu – Details	Alt + V and D
View Menu – Refresh	F5 or Alt + V and R
Tools Menu	Alt + O
Tool Menu – Notification	Alt + O and N
Tool Menu – Event Viewer	Alt + O and E
Tool Menu – Performance Monitor	Alt + O and r
Tool Menu – Options	Ctrl + O or Alt + O and P
Help Menu	Alt + H
Help Menu – Index	Alt + H and I
Help Menu – Using Help	Alt + H and U
Help Menu – Technical Support	Alt + H and T
Help Menu – Error Report	Alt + H and R
Help Menu – About CSAV for Exchange	Alt + H and A

MAIL ALERT VARIABLES

Mail alert messages in CSAV for Exchange use variables that are replaced by specific values when the mail alert message is generated. For example, the mail alert message specified in the following **Mail Alerts Configuration** dialog box contains four different variables: %SUBJECT%, %RECIPIENT%, %FILENAME%, and %VIRUSNAME%:



Mail Alerts Configuration Dialog Box

When a virus is detected, the variables in the message are replaced by the following values:

- %SUBJECT% - the subject of the e-mail message
- %RECIPIENT% - the name(s) of the intended e-mail recipient(s)
- %FILENAME% - the file name of the infected e-mail attachment
- %VIRUSNAME% - the name of the virus infecting the attachment

The mail alert message received by the sender of the infected e-mail would look similar to the following example:

```
The message Meeting Today you sent to John Smith has
the file attachment Program.zip which is infected with
the Sylvia virus.
```

You can use the following six different variables to create the mail alert message:

- %COMPUTERNAME% – the name of the CSAV for Exchange computer where the infection was found
- %FILENAME% – the file name of the infected e-mail attachment
- %RECIPIENT% – the name(s) of the intended e-mail recipient(s)
- %SENDER% – the name of the e-mail sender
- %SUBJECT% - the subject of the e-mail message
- %VIRUSNAME% – the name of the virus infecting the e-mail attachment

CSAV SERVICE STARTUP OPTIONS

Command AntiVirus for Exchange runs the **CSAV for Exchange Scheduler** service. Through the Windows 2000 **Services** dialog box, you can change the way the CSAV for Microsoft Exchange service starts. By default, the CSAV for Exchange service launches automatically when the Windows 2000 Server starts.



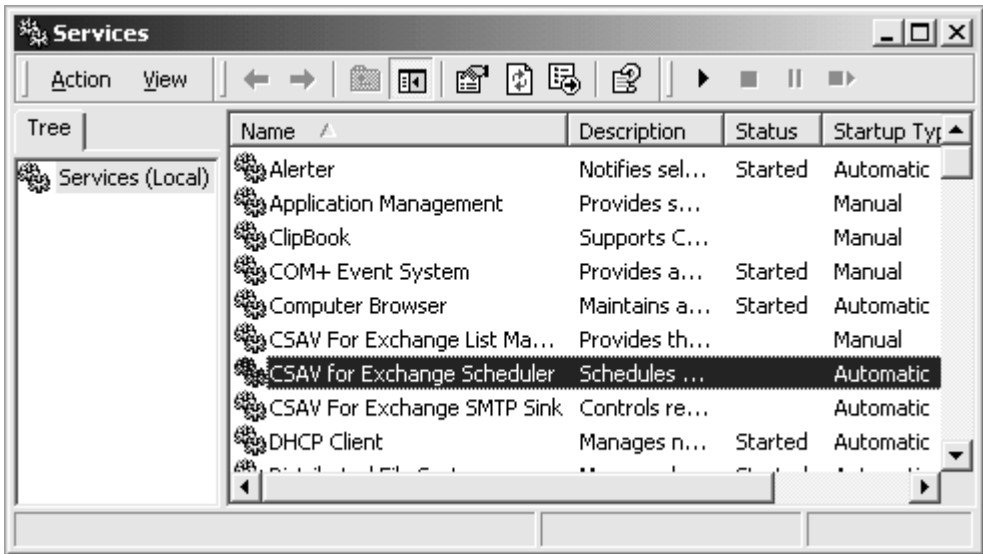
NOTE: The **on-access** service that provides real-time virus protection for your Exchange mail system is started automatically when the antivirus application programming interface (AVAPI) is loaded. The on-access service will **not** be listed in the Windows **Services** window.



To prevent accidental virus infection, we recommend that you do **not** change the default service startup options for CSAV for Exchange unless it is **absolutely** necessary.

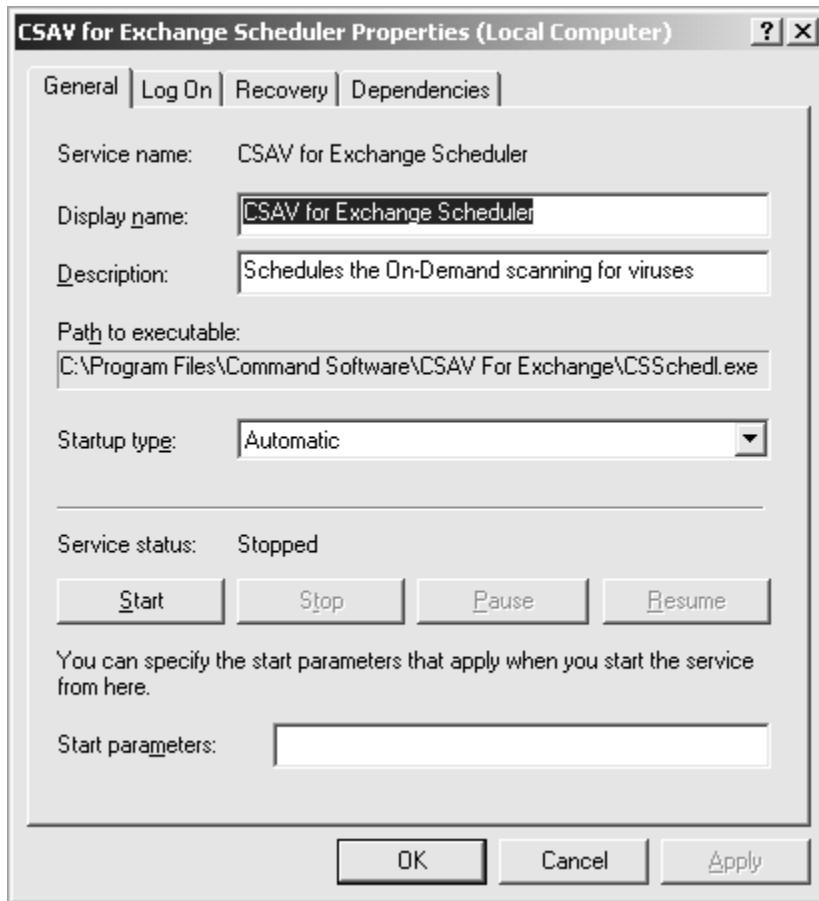
If you temporarily need to start or disable this service manually, follow these steps:

1. On the Windows taskbar, click the **Start** button.
2. Select **Settings**, and then click **Control Panel**. The system displays **Control Panel**.
3. Double-click **Administrative Tools**. The system displays the **Administrative Tools** window.
4. Double-click **Services**. The system displays the **Services** window:



Services Window

5. In the right pane, double-click **CSAV for Exchange Scheduler**. The system displays the **CSAV for Exchange Scheduler Properties** dialog box with the **General** dialog box in view:



General Dialog Box

6. In the **Startup type** list, select a startup type:

- **Automatic** - Starts the **CSAV for Exchange Scheduler** automatically at start up. This is the default option.
- **Manual** - Starts the **CSAV for Exchange Scheduler** service that you selected in **Step 5** only if you launch it manually after Windows 2000 starts.
- **Disabled** - Starts the service again only if you reset the service to **Manual** or **Automatic**.

7. Click **OK**.



There are three additional tabs, **Log On**, **Recovery**, and **Dependencies**, available on the **CSAV for Exchange Scheduler Properties** dialog box. To prevent accidental virus infection, we recommend that you do **not** change the default options in these dialog boxes unless it is **absolutely** necessary.

INDEX

A

- accessing Command AntiVirus 3-8
- Actions dialog box 3-27
- actions to take on infection 3-26
- activity logs 3-40
- additional information
 - help files 1-5
 - mailing list server 1-5
 - README.TXT 1-5
- administrator name 3-80
 - setting of 3-79
- Advanced dialog box 3-32
- alert messages
 - SMTP 3-79
- alerts
 - CSAV 3-56
- Automatic Update
 - configuring 4-3
 - directory 4-1
 - creating 4-2
 - specifying 4-5
 - immediate update 4-6
 - performing 4-6
 - scheduled download time 4-8
 - scheduling 4-6, 4-8
 - Update Now button 4-6
- Automatic Update dialog box 4-4

B

- Block Extensions dialog box 3-38
- Block Filename dialog box 3-37
- Block Subject dialog box 3-35
- blocking messages 3-34
- Browse Exchange Folders dialog box 3-18, 3-20, 3-46, 3-47
 - expanded view 3-19

- Browse for Folder dialog box 3-82
- buttons
 - command 3-5
 - toolbar 3-7

C

- chapter overviews 1-2
- Choose Administrator(s) dialog box 3-62, 3-81
- column headers 3-4
- Command AntiVirus
 - accessing 3-8
 - console 2-10, 3-1, 3-5
 - features 1-1
 - installing 2-1
 - removing 2-11
 - starting 2-10
- command buttons 3-5
- Command Software
 - mailing list server 1-5
 - technical support 1-4
 - Web Site 1-4
- complete installation 2-3
- compressed files 3-21, 3-24
- configuring scan task properties 3-16
- console
 - overview 2-10, 3-1, 3-2
 - using 3-5
- console for CSAV for Exchange, *see* CSAV for Exchange console
- conventions used 1-3
- copying a scan task 3-15
- copyright information 3-8, 3-83
- CSAV alerts 3-56

- CSAV for Exchange
 - options 3-79
 - product directory 4-2
 - CSAV for Exchange console 3-1
 - help menu 3-83
 - menu bar 3-7
 - status bar 3-54
 - task menu 3-11
 - tools menu 3-55
 - using 3-5
 - view menu 3-53
 - CSAV for Exchange Options dialog box 2-6, 3-80
 - CSAV On-demand Log File 3-52
 - CSAV On-demand Task Execution dialog box 3-12
 - CSAV Outbreak Actions dialog box 3-70
 - CSAV Outbreak Conditions dialog box 3-68
 - CSAV Outbreak Options dialog box 3-72
 - CSAV Outbreak Rules dialog box 3-67, 3-76
 - CSAV Outbreak Summary dialog box 3-74
 - CSAV services
 - Outbreak Manager 2-5
 - scheduler 2-5
 - SMTP Sink 2-5
 - CSAV shortcut menu 3-8
 - CSAVOnAccess.log 3-40
 - CSAVOnDemand.log 3-40
 - custom installation 2-3
 - customizing a scanning report 3-40
- D**
- deleting
 - infected items automatically 3-28
 - quarantined files 3-9
 - detection
 - on-access scan task properties 3-22
 - on-demand scan task properties 3-16
 - options 3-16
 - relationship to the exclusion feature 3-16, 3-44
 - Detection dialog box
 - on-access scan task 3-23
 - on-demand scan task 3-16
 - dialog boxes
 - Actions 3-27
 - Advanced 3-32
 - Automatic Update 4-4
 - Block Extensions 3-38
 - Block Filename 3-37
 - Block Subject 3-35
 - Browse Exchange Folders 3-18, 3-20, 3-46, 3-47
 - expanded view 3-19
 - Browse for Folder 3-82
 - Choose Administrator(s) 3-62, 3-81
 - CSAV for Exchange Options 2-6, 3-80
 - CSAV On-demand Task Execution 3-12
 - CSAV Outbreak Actions 3-70
 - CSAV Outbreak Conditions 3-68
 - CSAV Outbreak Options 3-72
 - CSAV Outbreak Rules 3-67, 3-76
 - CSAV Outbreak Summary 3-74
 - Detection
 - on-access scan task 3-23
 - on-demand scan task 3-16
 - Event Properties 3-65
 - Exclusion
 - on-demand scan task 3-45
 - File Extensions 3-21, 3-24
 - General A-6
 - Mail Alerts Configuration 3-61, A-3
 - Maintenance Complete 2-11
 - New File Extension 3-22, 3-25
 - Notification 3-60
 - Options 3-34
 - Outbreak Manager Settings 3-77
 - Reports 3-41
 - Schedule 4-7
 - on-demand scan task 3-43
 - Select activity log file 3-41
 - Select Features 2-4

- Select Service Start Options 2-4
- Setup Complete 2-8
- Setup Type 2-2
- Start Copying Files 2-5
- Task Statistics
 - on-demand scan task 3-49
- Update 4-4
- Welcome 2-2
- disinfection
 - of items automatically 3-28
 - of quarantined files 3-9
 - scan task statistics 3-50
- E**
- enabling the on-access scan 3-14
- error report 3-83
- errors
 - reporting of 3-83
- Event Properties dialog box 3-65
- Event Viewer
 - CSAV categories 3-64
 - running 3-8
 - using 3-64
- exclusion
 - of specific items from a scan task 3-44
 - relationship to the detection process 3-16, 3-44
- Exclusion dialog box
 - on-demand scan task 3-45
- extensions
 - default 3-21, 3-22, 3-24
 - scanning specific 3-21, 3-24
- F**
- features 1-1
 - quarantine 3-9
- file extensions
 - default 3-21, 3-22, 3-24
 - scanning specific 3-21, 3-24
- File Extensions dialog box 3-21, 3-24
- FTP site
 - configuring for downloads 4-5
 - primary 4-4, 4-5
 - secondary 4-4, 4-5
- full product updates 4-1
- G**
- General dialog box A-6
- getting started 2-10
- H**
- help
 - button 3-7
 - files 1-5
 - index 3-83
 - menu 3-83
 - using 3-83
- I**
- icons
 - accessing Command AntiVirus 3-8
 - changing size of 3-4
 - in the task list 3-3, 3-54
- installation, type of
 - complete 2-3
 - custom 2-3
- installing Command AntiVirus 2-1–2-9
- K**
- keyboard shortcuts A-1
- L**
- log files
 - CSAV On-demand 3-52
 - for a specific scan task 3-52
 - logging infections 3-27
 - logging options 3-42
 - Outbreak Manager
 - viewing of 3-77
 - saving reports 3-41
 - size 3-41
 - using View Log 3-40
 - viewing 3-40, 3-51, 3-52

M

- mail alert messages
 - additional addresses 3-63
 - canceling 2-7–2-8, 3-58
 - customizing 3-59
 - headers 3-60
 - sending to administrator 2-7–2-8, 3-58
 - sending to recipients 3-58
 - sending to sender 3-58
 - specifying an administrator 3-79
 - using variables 3-63, A-2
- Mail Alerts Configuration dialog box 3-61, A-3
- mailing list server 1-5
- Maintenance Complete dialog box 2-11
- menu
 - bar 3-2, 3-7
 - help 3-83
 - using 3-83
 - shortcut 3-6, 3-8
 - shortcut, CSAV 3-8
 - shortcut, Outbreak Manager 3-9
 - task 3-11
 - tools 3-55, 3-56
 - view 3-53
- messages
 - alert, SMTP 3-79
 - blocking 3-34
 - blocking by file extensions 3-38
 - blocking by file name 3-36
 - blocking by subject 3-35
 - fragmented
 - scan or block 3-39

N

- New File Extension dialog box 3-22, 3-25
- new task
 - button 3-5
 - creating 3-12

- notification
 - virus 3-58
 - customizing 3-59
- notification area shortcut menu 3-8
- Notification dialog box 3-60
- notifications 3-59, 3-79

O

- on-access scan task
 - changing properties 3-8
 - defining 3-3
 - detection options 3-22
 - disabling 3-14
 - enabling/disabling 3-6, 3-8
 - mail attachments to scan 3-23, 3-24
 - statistics 3-48, 3-50
 - updating status 3-54
- on-demand scan task
 - copying 3-15
 - defining 3-3
 - detection properties 3-16
 - items to scan 3-16
 - performing scans automatically 3-42
 - starting 3-12, 3-13
 - statistics 3-49
 - updating status 3-54
- Options dialog box 3-34
- Outbreak Manager
 - actions 3-69
 - conditions 3-67
 - configuration rules 3-66
 - icon 3-9, 3-66
 - settings 3-77
 - shortcut menu 3-9
 - summary of rules 3-73
- Outbreak Manager log 3-78
- Outbreak Manager service
 - selection of 2-5
- Outbreak Manager Setting dialog box 3-77
- overview
 - chapters 1-2

P

product directory 4-2

Q

quarantine

feature 3-9

folder 3-10

setting of 3-79

specifying 2-8

infected items automatically 3-27

R

README.TXT 1-5, 2-9

removing Command AntiVirus 2-11

renaming a scan task 3-14

report

error 3-83

reports

customizing 3-40

types of information to be logged 3-42

Reports dialog box 3-41

S

scan engine information 3-83

scan statistics

last scan results 3-50

resetting 3-8

viewing 3-8

scan task

action to take on infection 3-26, 3-27

activity log 3-40

changing icon size 3-4

changing name of 3-4

configuring properties of 3-16

copying 3-15

creating new 3-12

deleting 3-14

editing 3-15

enabling/disabling on-access 3-14

excluding items from 3-44

items to scan 3-16, 3-17

on-access

advanced settings for 3-31

command buttons 3-5

configuring 3-22

defining 3-3

enabling/disabling 3-8, 3-14

icon 3-3

on-demand

command buttons 3-5

configuring 3-16

defining 3-3

icon 3-3

starting 3-12

Task Execution Window 3-13

performing scans automatically 3-42

renaming of 3-4, 3-14

schedule scan frequency 3-43

scheduling 3-42

sort order of 3-4

starting 3-12

statistics, viewing of 3-48

task menu 3-11

type of 3-3

updating status 3-54

views of 3-4

Schedule dialog box 4-7

on-demand scan task 3-43

scheduled scans

definition 3-3

scheduling 3-42, 3-43

scheduler service 2-5, A-4

selection of 2-5

scheduling

scans 3-42

scheduling automatic updates 4-8

Select activity log file dialog box 3-41

Select Features dialog box 2-4

Select Service Start Options dialog box 2-4

service start options

selecting of 2-4

service startup options A-4

Services window A-5

- Setup Complete dialog box 2-8
 - Setup Type dialog box 2-2
 - shortcut menu 3-6
 - CSAV 3-8
 - defining 3-6
 - notification area 3-8
 - Outbreak Manager 3-9
 - SMTP
 - alert messages 3-79
 - Sink service
 - selection of 2-5
 - staging directory
 - definition 4-1
 - Start Copying Files dialog box 2-5
 - starting
 - an on-demand scan task 3-12
 - Command AntiVirus 2-10
 - the on-access scan task 3-14
 - statistics
 - viewing 3-48
 - status bar 3-54
 - turning on and off 3-53, 3-54
 - stopping
 - the on-access scan task 3-14
 - system information 3-83
 - system requirements 1-4
- T**
- task list
 - about 3-2
 - changing appearance 3-53
 - configuring scan tasks from 3-12
 - defining 3-2
 - deleting scan task from 3-14
 - icons 3-54
 - new task 3-5
 - on-access scan 3-3
 - on-demand scan 3-3
 - sort order of scan tasks 3-4
 - viewing 3-4
 - task menu 3-11
 - on-demand scan task 3-11
 - task names 3-2
 - Task Statistics dialog box
 - on-demand scan task 3-49
 - task window 3-2, 3-3
 - defining 3-2
 - resizing column headers 3-4
 - updating status of scan tasks 3-54
 - technical support 1-4, 3-83
 - toolbar
 - accessing Event Viewer 3-64
 - buttons 3-7
 - turning on and off 3-53
 - tools menu 3-56
 - Automatic Update 3-55
 - CSAV Alerts 3-55
 - Event Viewer 3-55
 - Notification 3-55
 - Options 3-55
 - Outbreak Manager 3-55
 - Performance Monitor 3-55
- U**
- Universal Naming Convention (UNC) 4-2
 - Update dialog box 4-3, 4-4
- V**
- version number 3-8, 3-83
 - view menu
 - using 3-53
 - virus
 - actions to take 3-26, 3-28
 - notification
 - customizing 3-59
 - notifications 3-58, 3-79
- W**
- Welcome dialog box 2-2
 - window
 - Services A-5
 - task 3-2, 3-3