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.

**Published in the U.S.A. by Command Software Systems, Inc. All rights reserved.
Document No. CME-244-0401**

Part No. 07-1400-00

TABLE OF CONTENTS

INTRODUCTION

Congratulations on choosing Command AntiVirus™ for Microsoft® Exchange for outstanding security against e-mail-based computer viruses! Command AntiVirus provides you with the latest technology for preventing the spread of computer viruses through your Microsoft Exchange network. To receive the latest information on updates and new releases, please take a moment to register your product.

MAIN FEATURES

Command AntiVirus (CSAV) for Microsoft Exchanges a comprehensive anti-virus 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 NT service and provides NT 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.

- Performs continuous background scanning.
- Uses easy to understand configuration options.

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 covers the product's installation, uninstall, and reinstallation procedures.

Chapter 3 - Using Command AntiVirus

This chapter provides information on creating custom scans, setting scan properties, and scheduling automatic scans. You will also find advice on configuration settings, toolbar items, and menu bar options.

Chapter 4 - Automatic Update

Chapter 4 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

The glossary defines the terms that you need for a solid understanding of anti-virus systems.

Appendix

This chapter gives a complete listing of all the keyboard shortcuts that are available in CSAV. The chapter 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
```

KEY + KEY The plus (+) sign between two keys indicates pressing both keys at the same time. For example, when asked to press CTRL+C, press and hold the control key, and then press the letter “c” key.

CSAV The acronym used for Command AntiVirus.

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 NT® Server 4.0 with Service Pack 3 or higher
- Microsoft® Exchange Server Release 5.5 with Service Pack 3 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 system security? Would you like to know the answers to our customers' most frequently asked questions? We provide comprehensive information on viruses, products, events, employment opportunities and much more. Plus, for your convenience, all of our readme files, quick start guides, and manuals are available for online viewing.

Be sure to visit this exciting extension of Command Software Systems' services at **www.commandsoftware.com** or our web site in the United Kingdom at **www.command.co.uk**.

HELP FILES

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

MAILING LIST SERVER

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

README.TXT

The latest information on product enhancements, fixes and special instructions is in the README.TXT file that is included with the CSAV program files. 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 very 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 version 5.0 or higher is running on your server.

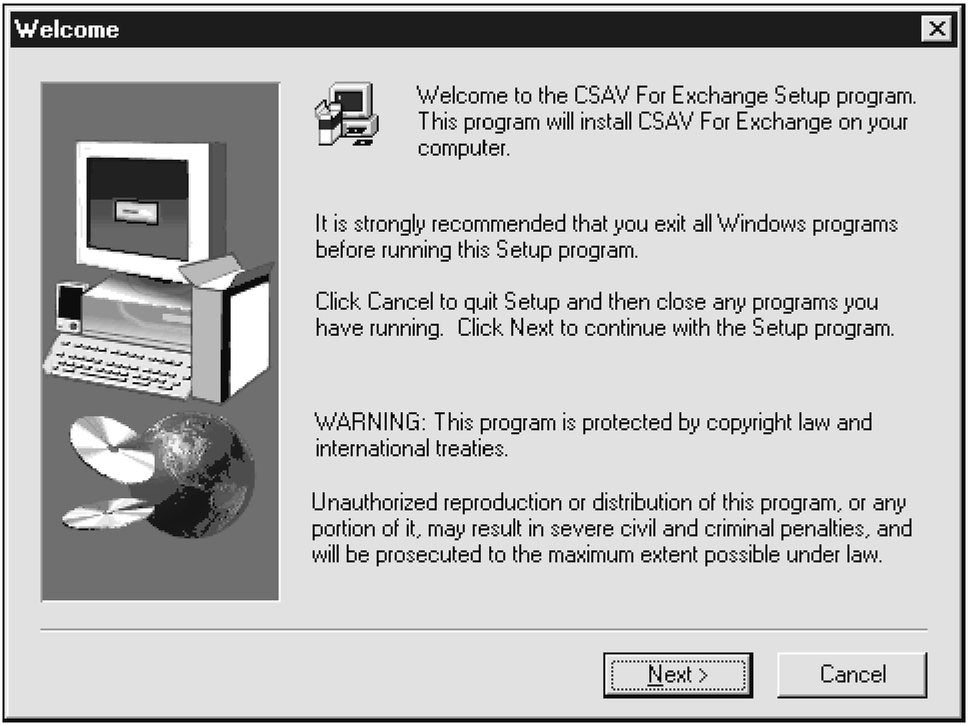
Also, make sure that you are logged on as:

A. an administrator on the local domain.

B. an Exchange Server administrator. This account should be the one on which the Exchange services run.

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

1. Insert the CD-ROM.
2. Click the **Start** button.
3. Click **Run**.
4. Select **Browse** to search the CD for the **EXCHANGE** directory.
5. Change to that directory.
6. Double-click **Setup.exe** and click **OK**. After startup, the system displays the **Welcome** dialog box.



Welcome to the CSAV For Exchange Setup program. This program will install CSAV For Exchange on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

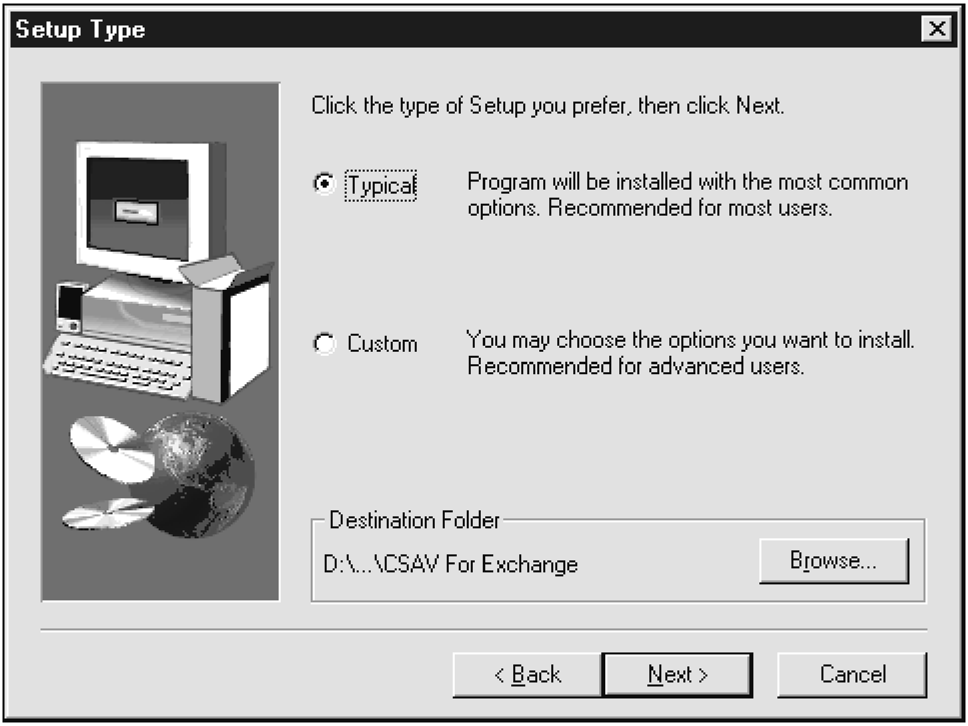
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

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

Click the type of Setup you prefer, then click Next.

● Typical Program will be installed with the most common options. Recommended for most users.

○ Custom You may choose the options you want to install. Recommended for advanced users.

Destination Folder

D:\...\CSAV For Exchange

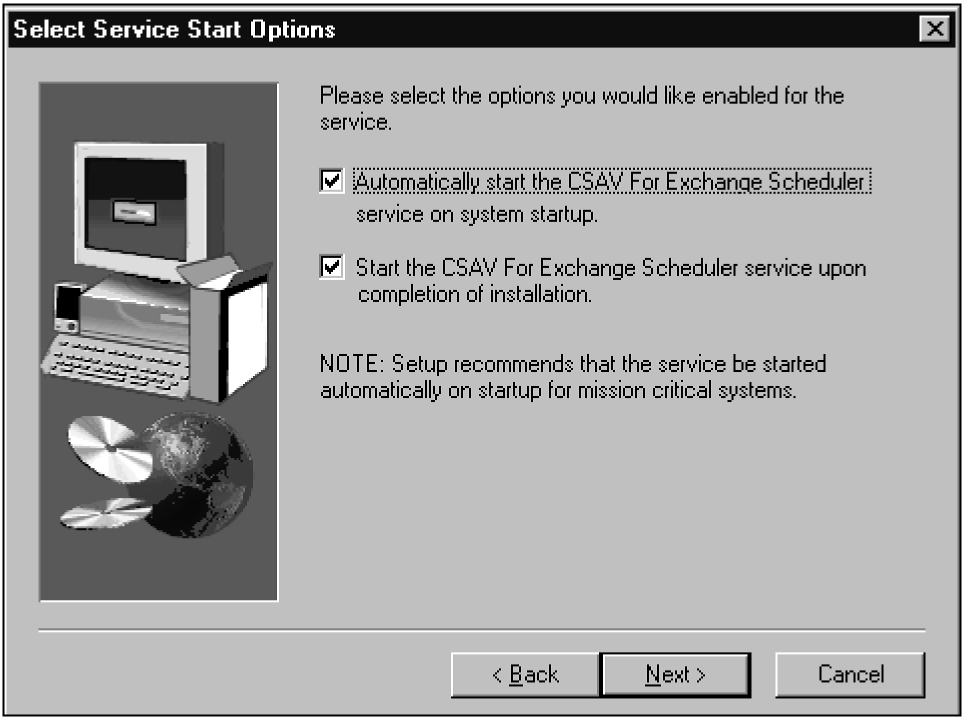
Setup Type Dialog Box

9. Select **one** of the following installations. We recommend the **Typical** installation.

   - **Typical –** 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

Please select the options you would like enabled for the service.

☑ Automatically start the CSAV For Exchange Scheduler service on system startup.

☑ Start the CSAV For Exchange Scheduler service upon completion of installation.

NOTE: Setup recommends that the service be started automatically on startup for mission critical systems.

Select Service Start Options Dialog Box

This dialog box allows you to select the startup options for the **Scheduler** service. The **Scheduler** service allows you to schedule virus scans.

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

Select from the following options:

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

We recommend that you select both options. This is the default setting.

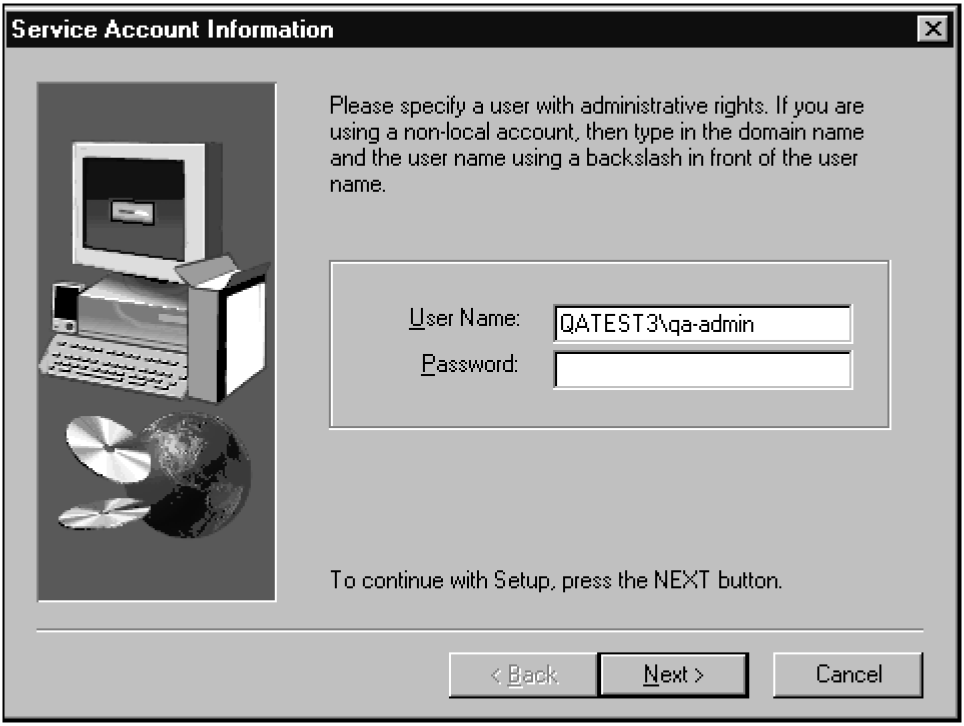
12. Click **Next**. The system displays the **Start Copying Files** dialog box.

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

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

    When the copying is complete, the system displays the **Service Account Information** dialog box.

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



Service Account Information

Please specify a user with administrative rights. If you are using a non-local account, then type in the domain name and the user name using a backslash in front of the user name.

User Name: QATEST3\qa-admin

Password:

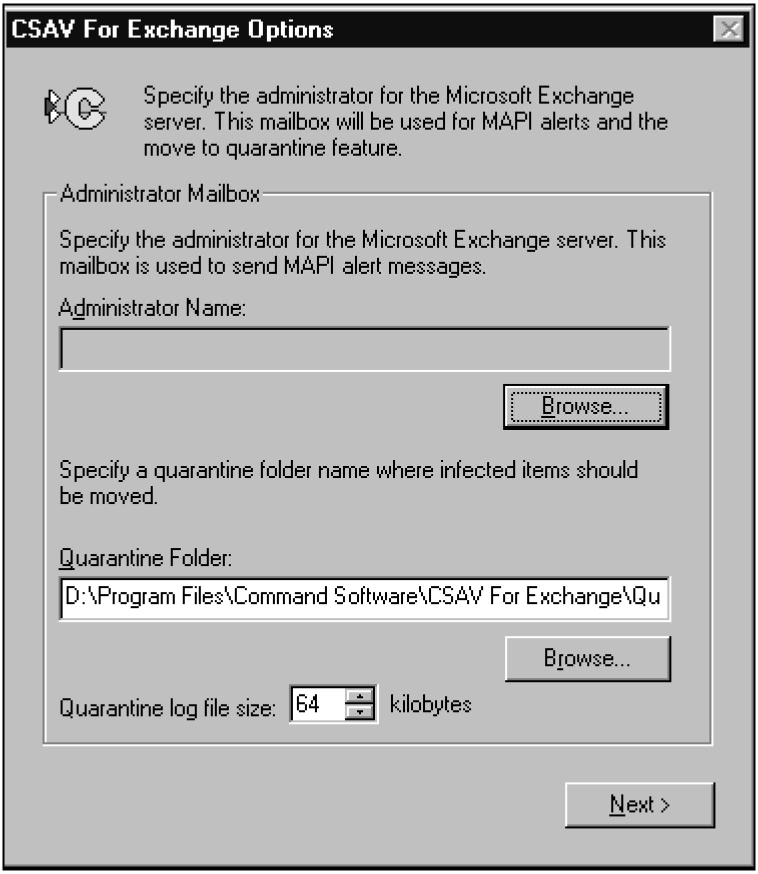
To continue with Setup, press the NEXT button.

Service Account Information Dialog Box

14. Type the user name's password in the **Password** text box. This identifies the Windows NT account under which the Command AntiVirus services run.

NOTE: If you did not use the correct user name, the system displays a dialog box that informs you that you have entered the wrong user name. The user name should be the user name that installed Exchange Server.

15. Click **Next**. The system displays the **CSAV for Exchange Options** dialog box:



CSAV For Exchange Options

Specify the administrator for the Microsoft Exchange server. This mailbox will be used for MAPI alerts and the move to quarantine feature.

Administrator Mailbox

Specify the administrator for the Microsoft Exchange server. This mailbox is used to send MAPI alert messages.

Administrator Name:

Browse...

Specify a quarantine folder name where infected items should be moved.

Quarantine Folder: D:\Program Files\Command Software\CSAV For Exchange\Qu

Browse...

Quarantine log file size: 64 kilobytes

Next >

CSAV for Exchange Options Dialog Box

16. Use the **Browse** button to select an **Administrator Name.**

    If 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.

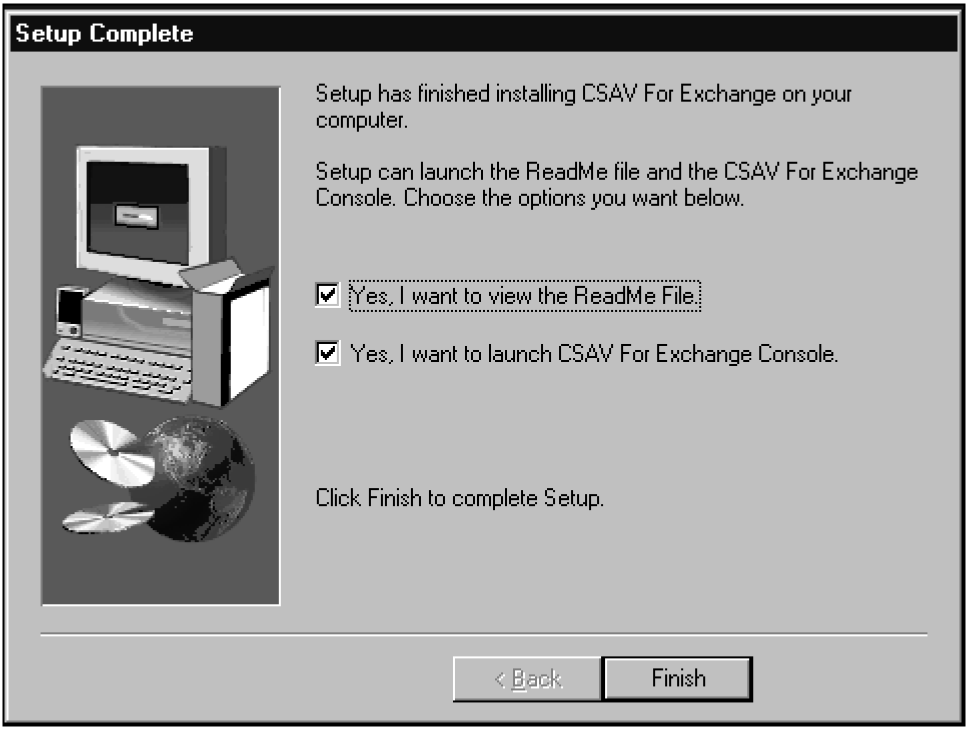
    You can also change the Exchange mail folder that holds infected files in quarantine. The default is `Program Files\Command Software\CSAV for Exchange\Quarantine`. To change the **Quarantine Folder**, use the **Browse** button to select a folder from the **Browse for Folder** dialog box.

17. After you have selected the **Administrator Name** and the **Quarantine Folder**, click **Next**. The system displays a dialog box containing the following message:

    THE ACCOUNT HAS BEEN GRANTED THE "LOG ON AS A SERVICE" RIGHT.

    This right is required for the account to run the service.

18. Click **OK**. The system displays the **Setup Complete** dialog box:



Setup Complete

Setup has finished installing CSAV For Exchange on your computer.

Setup can launch the ReadMe file and the CSAV For Exchange Console. Choose the options you want below.

☑ Yes, I want to view the ReadMe File.

☑ Yes, I want to launch CSAV For Exchange Console.

Click Finish to complete Setup.

Setup Complete Dialog Box

19. 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.
20. 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 NT taskbar, click the **Start** button.
2. Select **Programs**.
3. Select **Command Software**.
4. Select **CSAV for Exchange**.
5. Click the **CSAV for Exchange Console** icon. The system displays the **CSAV for Exchange Console**.

CSAV FOR EXCHANGE CONSOLE

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

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

REMOVING COMMAND ANTIVIRUS

To remove Command AntiVirus for Microsoft Exchange follow these directions.

To uninstall CSAV for Exchange from a Windows NT 3.51 server, use the uninstallation icon in the CSAV for Exchange program group.

1. On the Windows NT taskbar, click the **Start** button.
2. Select **Settings**.
3. Click **Control Panel**.
4. Double-click the **Add/Remove Programs** icon.
5. Click the **Install/Uninstall** tab.
6. Select **CSAV for Exchange** from the list of installed applications.
7. Click the **Add/Remove** button. The system displays the **Confirm File Deletion** message box.
8. Click **Yes**. The system displays the **Remove Programs From Your Computer** dialog box.
9. Click **OK**. The system displays a confirmation message box that recommends you restart your system. A system restart is required to completely remove CSAV for Exchange.
10. Click **OK**. The system displays a message box asking if you want to restart now.

    To restart your computer now, click **Yes**.

    To restart at a later time, click **No**, and then click **OK** to exit.

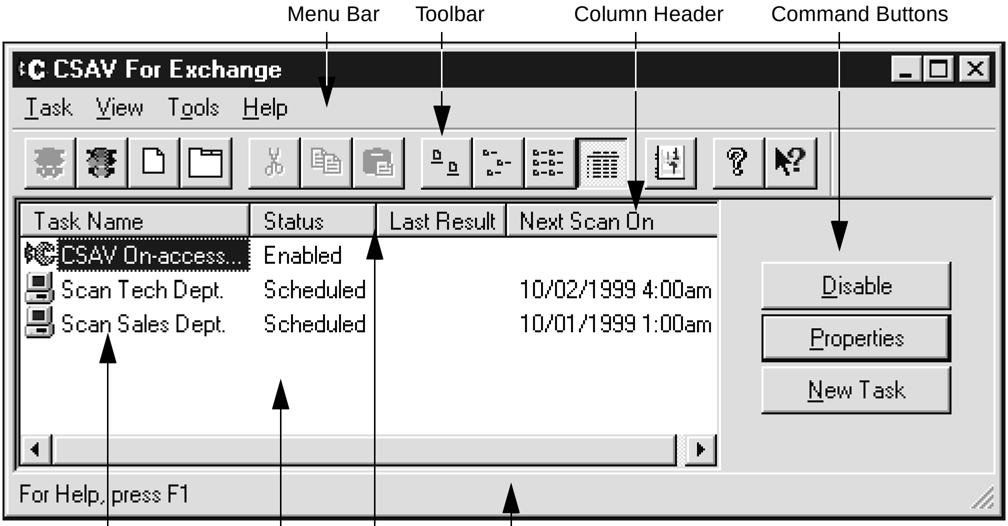
To remove CSAV for Exchange completely, you must restart your server.

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**.



Task Name	Status	Last Result	Next Scan On
CSAV On-access...	Enabled		
Scan Tech Dept.	Scheduled		10/02/1999 4:00am
Scan Sales Dept.	Scheduled		10/01/1999 1:00am

For Help, press F1

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 from the console.

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 toolbar, 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.

The console’s status bar displays the current state of a scan action. For example, if you start an on-demand scan, the status bar informs you that the scan is running.

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 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

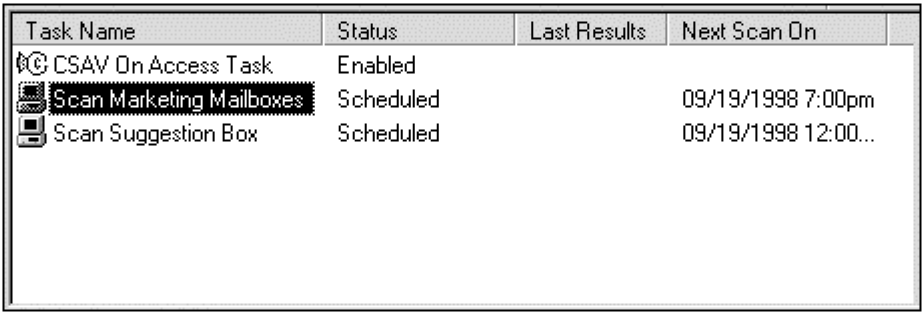
You can create and configure scan tasks from the **Task List**. For example, you can set properties for tasks and specify which actions to use upon detecting a virus. You can also create an activity log file, schedule scan tasks to run automatically and more.

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 sizes.

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

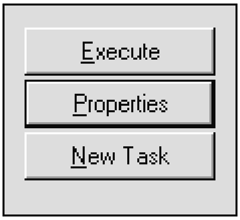
To change a scan task name, click its name in the **Task List**, pause, and click again. Then, type the new name for the scan task. You can also use the right mouse button (right-click) to click a scan task name and then select **Rename** from the shortcut menu. If you make an error while typing in a 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. Highlight the scan task you want to run or modify. Then, select the appropriate command button. For example, clicking the **Execute** button starts an on-demand scan. Clicking the **Properties** button allows you to access the scan task configuration features.



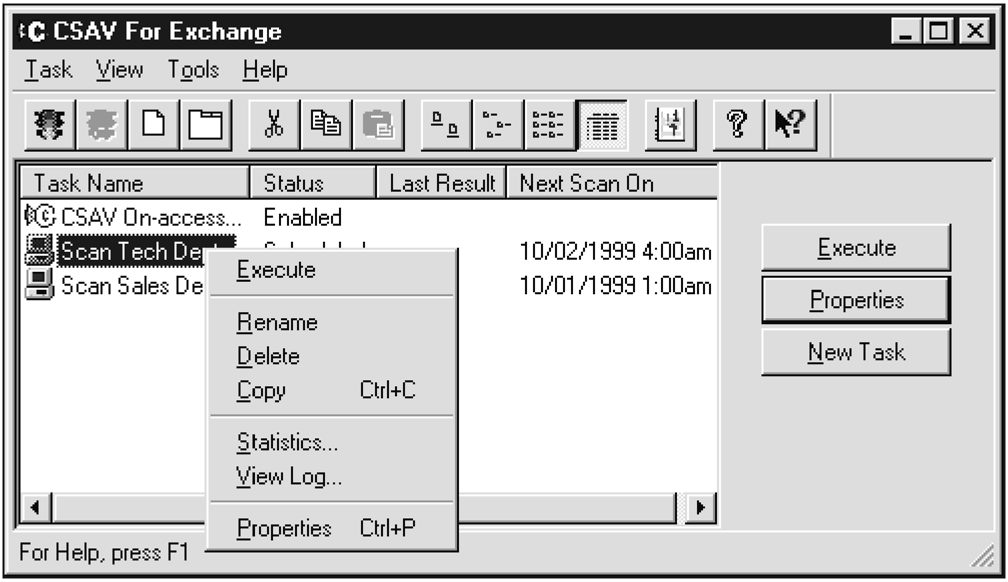
Command Buttons

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 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. Performing a right-mouse click anywhere in the **Task Window** brings up a shortcut menu:



Task Name	Status	Last Result	Next Scan On
CSAV On-access...	Enabled		
Scan Tech De			10/02/1999 4:00am
Scan Sales De			10/01/1999 1:00am

Shortcut Menu

Items available on the shortcut menus vary depending on whether you selected the on-access scan task name, an on-demand scan task name or performed a right-click in a blank area in the **Task Window**. For example, if you right-click the on-access scan task name, the system displays a shortcut menu containing the **Enable**/**Disable**, **Statistics**, **View Log**, and **Properties**. If you right-click an on-demand scan task name, the system displays a shortcut menu containing the **Execute**, **Rename**, **Delete**, **Copy**, **Statistics**, **View Log**, and **Properties** items.

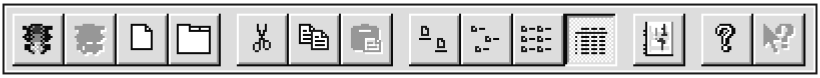
If an item on a shortcut menu is not available, it appears dimmed.

MENU BAR

The menu bar in the **CSAV for Exchange console** contains **Task**, **View**, **Tools**, and **Help** menus that you can access with a mouse or keyboard. 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.

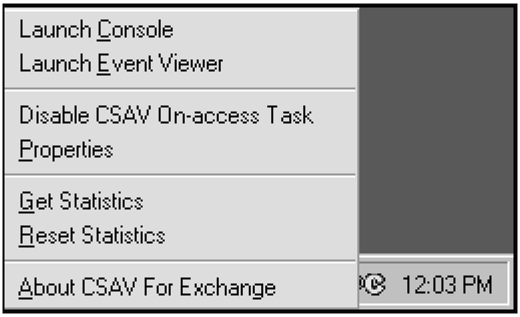
From the **View** menu, you can turn on or turn off the toolbar as needed.

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.

OTHER WAYS TO ACCESS PROGRAM FEATURES

You can use the **C** icon in the system tray 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 **Tray Shortcut Menu**:



Tray Shortcut Menu

The tray shortcut menu allows you to:

- Open the **CSAV for Exchange console**
- Run 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

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 and extension with **.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 later in this chapter.

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, see **Options** in **Using the Tools Menu** located later in this chapter.

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, see **Action to Take on Infection** in **Configuring Scanning Properties** located later in this chapter.

QUARANTINE LOG FILE

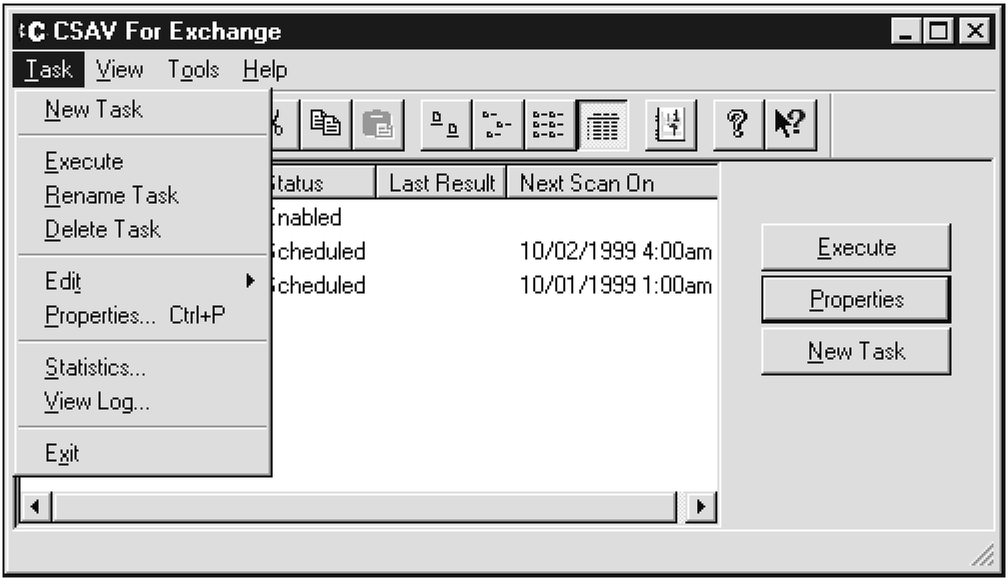
If files have been moved to the quarantine folder, corresponding entries for these files are added to the quarantine log file. This log file is named **History.log**. It is found in the **CSAV for Exchange** installation folder. The **History.log** file provides information on the following:

- The original location of the e-mail
- The host name of the computer that was running CSAV for Exchange
- The name of the user under which CSAV for Exchange was running
- The date and time the log file was created or modified
- The subject of the e-mail
- The name of the quarantined attachment
- Whether the attachment was successfully quarantined

If a file attachment name is not found, the default file attachment name of **(Unknown)** is assigned.

USING THE TASK MENU

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



Status	Last Result	Next Scan On
Enabled		
Scheduled		10/02/1999 4:00am
Scheduled		10/01/1999 1:00am

Task Menu (On-demand)

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
- **Rename** a scan task
- **Delete** a 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 scan task, select the **Task** menu and click the **New Task** menu item. This creates a new scan task called **New Scan Task** at the bottom of the **Task List**.

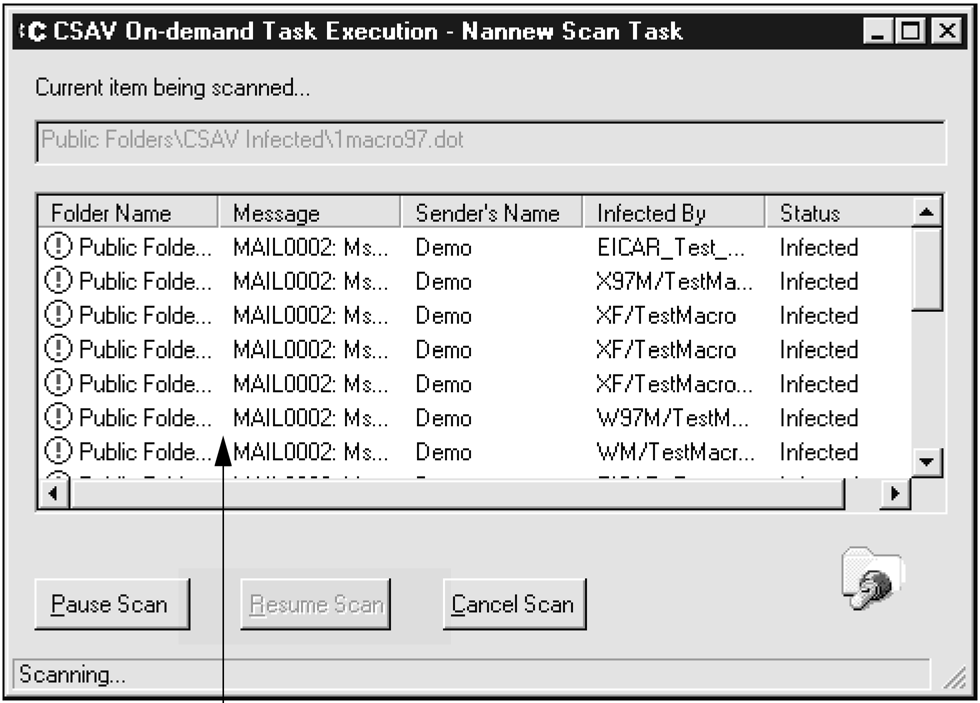
You can change the name of the new scan task by typing in the new name and pressing **Enter** to save the change.

To configure the scanning characteristics of the scan task, select the scan task name from the **Task List**. Then, select the **Task** menu and click the **Properties** menu item.

For more information, see **Configuring Scanning Properties** located later in this chapter.

EXECUTING A SCAN

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



CSAV On-demand Task Execution - Nannew Scan Task

Current item being scanned...

Public Folders\CSAV Infected\1macro97.dot

Folder Name	Message	Sender's Name	Infected By	Status
Public Folde...	MAIL0002: Ms...	Demo	EICAR_Test_...	Infected
Public Folde...	MAIL0002: Ms...	Demo	X97M/TestMa...	Infected
Public Folde...	MAIL0002: Ms...	Demo	XF/TestMacro	Infected
Public Folde...	MAIL0002: Ms...	Demo	XF/TestMacro	Infected
Public Folde...	MAIL0002: Ms...	Demo	XF/TestMacro...	Infected
Public Folde...	MAIL0002: Ms...	Demo	W97M/TestM...	Infected
Public Folde...	MAIL0002: Ms...	Demo	WM/TestMacr...	Infected

Scanning...

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 files that are being scanned. As files are scanned in real-time, the names displayed in this text box change quickly.

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

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

- **Sender's Name** – Contains the names of the individuals who sent 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**. Then, select the **Task** menu and click either the **Enable** or **Disable** menu item.

RENAMING A SCAN TASK

To rename a scan task, select the task's name in the **Task List**. Then, select the **Task** menu and click the **Rename Task** menu item. 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**. Then, select the **Task** menu and click the **Delete Task** menu item.

NOTE: The on-access scan task is a permanent feature in CSAV. It can be configured, but it cannot be 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 **Copy of Scan Marketing Inbox** is created in the **Task List**.
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, see **Configuring Scanning Properties** located later in this chapter.

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**. Except for **Schedule and Exclusion**, the same dialog boxes are available for the on-access scan. 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**, **Reports**, **Schedule**, and **Exclusion** dialog boxes to configure the on-access scan and on-demand scans.

Detection Options

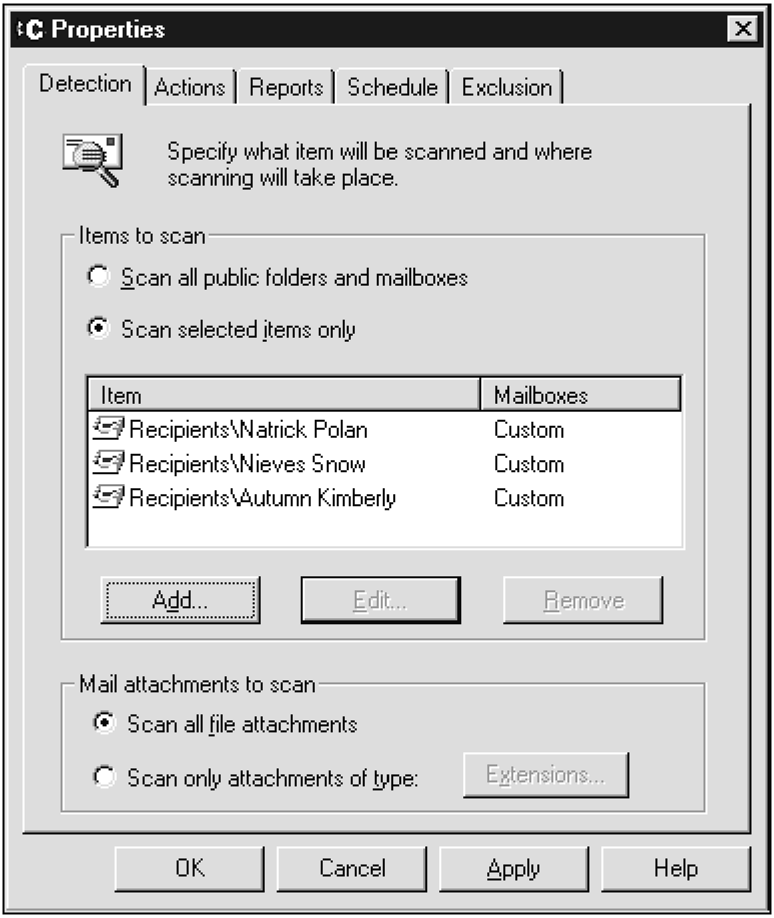
The **Detection** dialog box allows you to select which mailboxes, folders, and types of attachments to scan.

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 visible:



Specify what item will be scanned and where scanning will take place.

Items to scan

○ Scan all public folders and mailboxes

● Scan selected items only

Item	Mailboxes
Recipients\Natrick Polan	Custom
Recipients\Nieves Snow	Custom
Recipients\Autumn Kimberly	Custom

Mail attachments to scan

● Scan all file attachments

○ Scan only attachments of type:

Detection Dialog Box (On-demand)

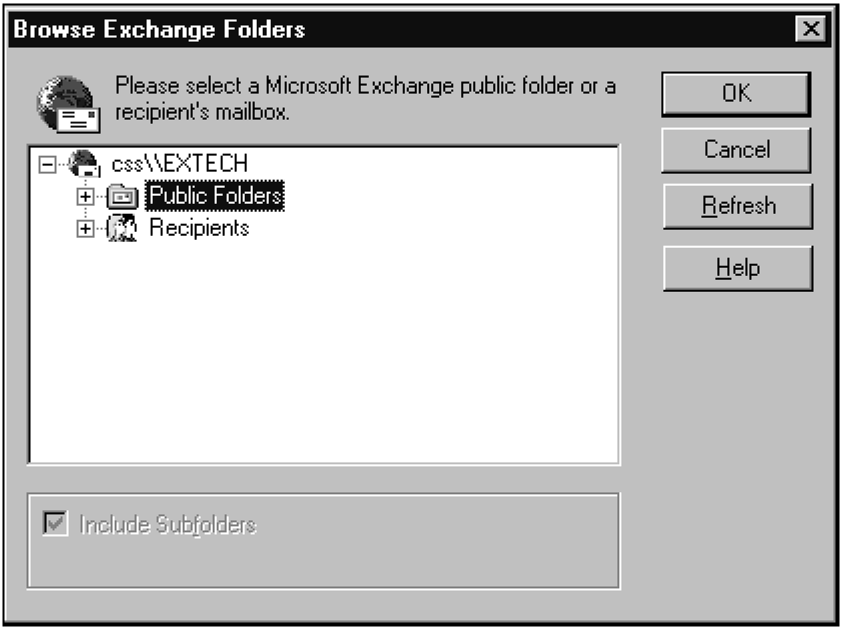
4. In **Items to scan**, select **one** of the following:

   - **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

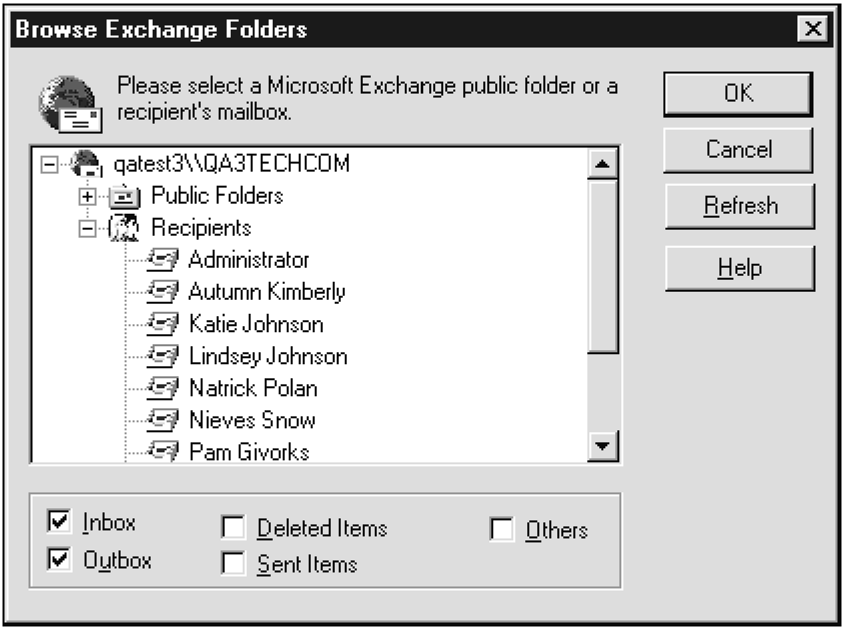
Please select a Microsoft Exchange public folder or a recipient's mailbox.

css\\EXTECH
Public Folders
Recipients

☑ Include Subfolders

Browse Exchange Folders Dialog Box

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



Browse Exchange Folders

Please select a Microsoft Exchange public folder or a recipient's mailbox.

- qatest3\\QA3TECHCOM
  - Public Folders
  - Recipients
    - Administrator
    - Autumn Kimberly
    - Katie Johnson
    - Lindsey Johnson
    - Natrick Polan
    - Nieves Snow
    - Pam Givorks

☑ Inbox
☑ Outbox
□ Deleted Items
□ Sent Items
□ Others

Browse Exchange Folders Dialog Box – Expanded View

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** – you can also choose to scan subfolders. To scan subfolders select the **Include Subfolders** check box.

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

- If you select a mailbox – the mail item check boxes (**Inbox**, **Outbox**, **Deleted Items**, **Sent Items**, and **Others**) are available for each mailbox. This feature allows you to select different items for each mailbox. Select the mail items that you want included in the scan.

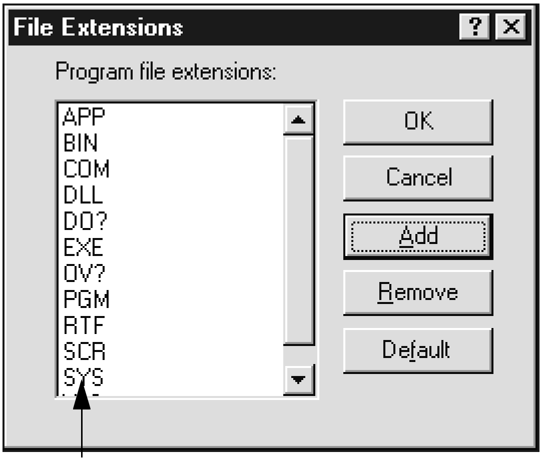
NOTE: If you select multiple single files and/or folders or a block of files and/or folders, the mail item check boxes are only available for the total selection. The mail item check boxes that you select apply to **all** of the files and/or folders that you selected.

7. Click **OK** to add the selected folders and return to the **Detection** dialog box.
8. In **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 11**.
- **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** and **AR?** 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.



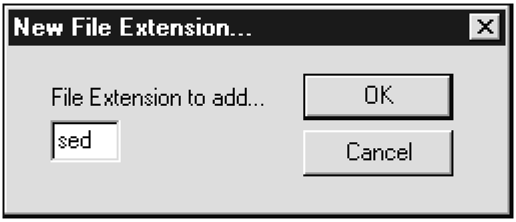
Program file extensions:

- APP
- BIN
- COM
- DLL
- DO?
- EXE
- OV?
- PGM
- RTF
- SCR
- SYS

File Extensions List **File Extensions Dialog Box**

9. 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:



File Extension to add... sed

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.

10. Click **OK**.
11. In the **Detection** dialog box, click **OK** to save your changes.

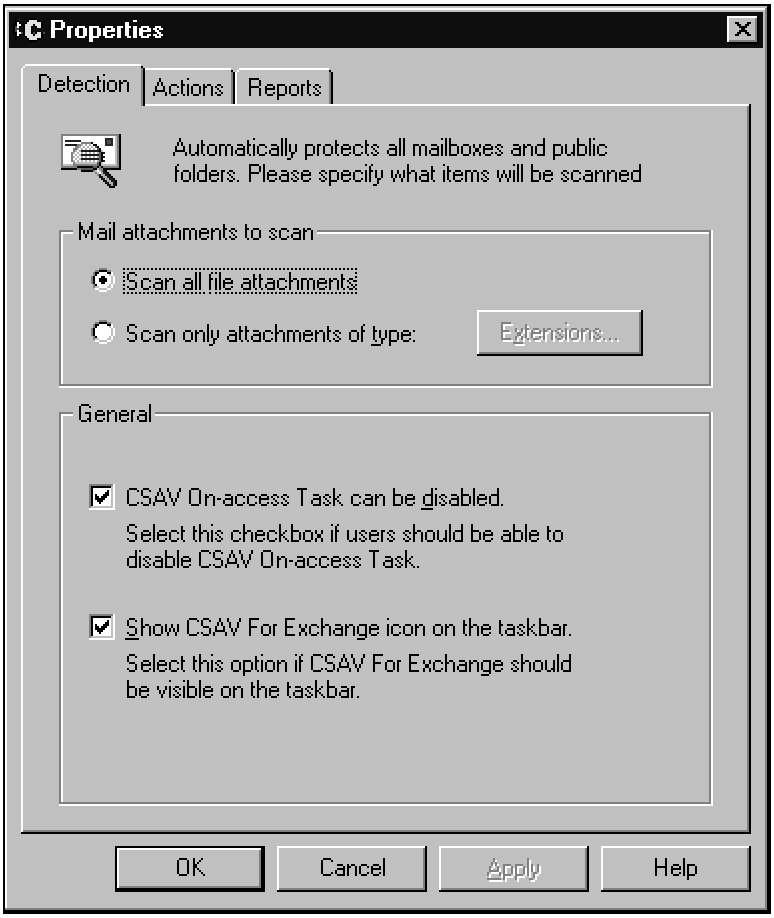
The **Default** button in the **File Extensions** dialog box resets the list to the default extensions. Any file extensions you added are lost.

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 visible:



Automatically protects all mailboxes and public folders. Please specify what items will be scanned

Mail attachments to scan

● Scan all file attachments

○ Scan only attachments of type:

General

☑ CSAV On-access Task can be disabled.

Select this checkbox if users should be able to disable CSAV On-access Task.

☑ Show CSAV For Exchange icon on the taskbar.

Select this option if CSAV For Exchange should be visible on the taskbar.

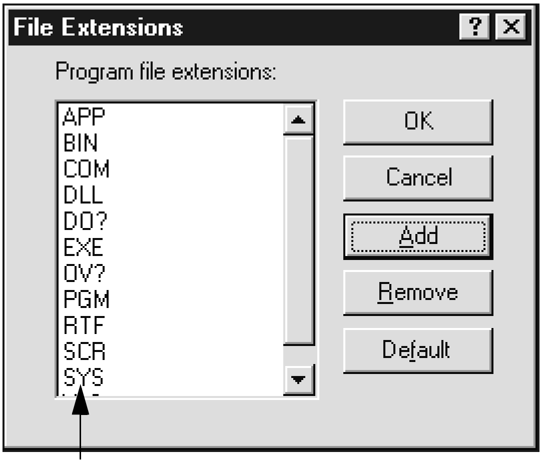
Detection Dialog Box (On-access)

4. In **Mail attachments to scan**, select **<u>one</u>** 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 7**.

- **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** and **AR?** 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.

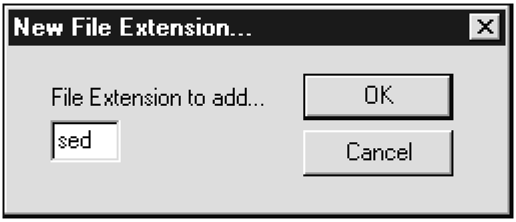


APP
BIN
COM
DLL
DO?
EXE
OV?
PGM
RTF
SCR
SYS

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:



File Extension to add... sed

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, select one or more of the following:

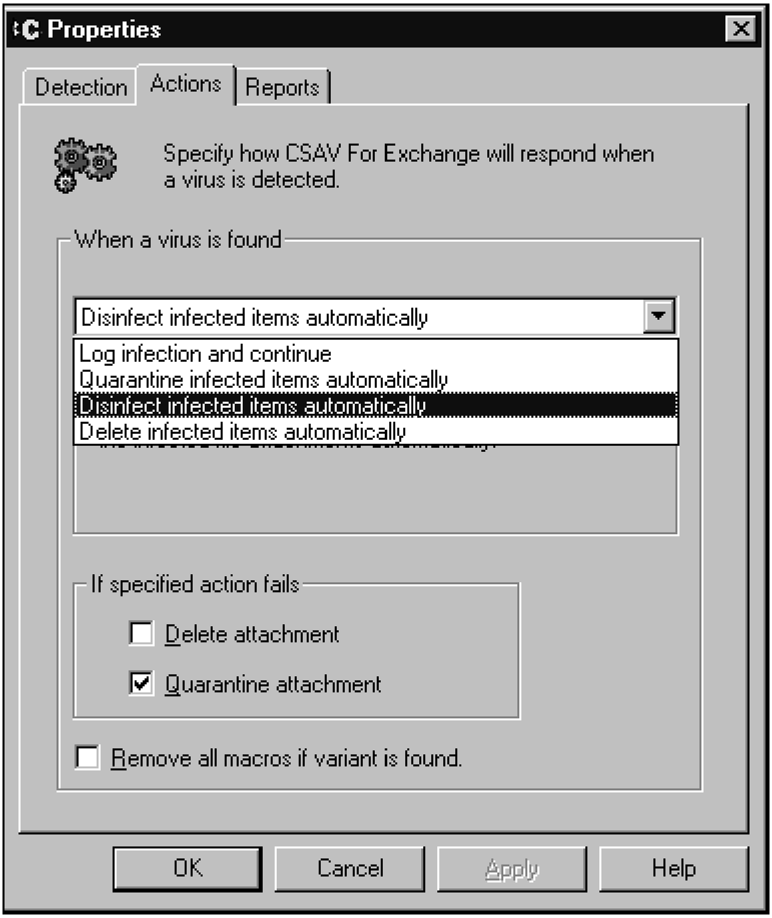
- **CSAV On-access Task can be disabled** – If selected, allows users at the server running CSAV for Exchange to turn off the on-access scan task. The on-access scan task can then be disabled (or reenabled) using the **Enable**/**Disable** command that is available from the **CSAV for Exchange console**. 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 Windows system tray. 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 the **Properties**. The system displays the **Properties** dialog box.
4. Click the **Actions** tab. The system displays the **Actions** dialog box:



Specify how CSAV For Exchange will respond when a virus is detected.

When a virus is found

Disinfect infected items automatically

Log infection and continue
Quarantine infected items automatically
Disinfect infected items automatically
Delete infected items automatically

If specified action fails

□ Delete attachment

☑ Quarantine attachment

□ Remove all macros if variant is found.

Actions Dialog Box

5. In **When a virus is found**, click the drop-down-arrow and select **<u>one</u>** 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 and extension with **.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 later in this chapter.

NOTE: When an infected file is moved to the **Quarantine** folder, it is renamed. For more information, refer to **Using the Quarantine Feature** located previously in this chapter.

- **Disinfect infected items automatically –** Disinfects attachments. The attachments are disinfected 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, you can also select the **Remove all macros if variant is found** option at the bottom of the dialog box. This option removes all macros from the infected attachment if a variant of an existing macro virus is found.

- **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 and extension with **.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 later in this chapter.

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 **<u>one</u>** 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 and extension with **.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 later in this chapter.

- **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 and extension with **.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 later in this chapter.

NOTE: When an infected file is moved, it is renamed. For more information, refer to **Using the Quarantine Feature** located previously in this chapter.

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

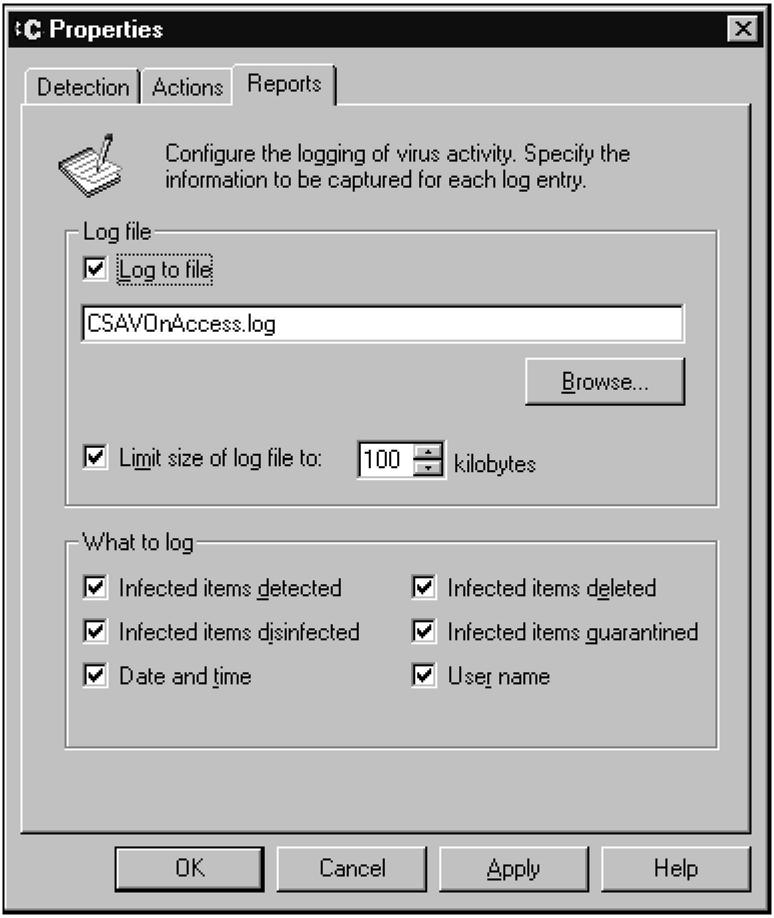
Reports

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, 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** and then select **View Log** from the **Task** menu. 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:



Configure the logging of virus activity. Specify the information to be captured for each log entry.

Log file

☑ Log to file

CSAVOnAccess.log

☑ Limit size of log file to: 100 kilobytes

What to log

☑ Infected items detected ☑ Infected items deleted

☑ Infected items disinfected ☑ Infected items quarantined

☑ Date and time ☑ User name

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 **64KB**; 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 NT system running CSAV for Exchange.
8. Click **OK** to save your changes.

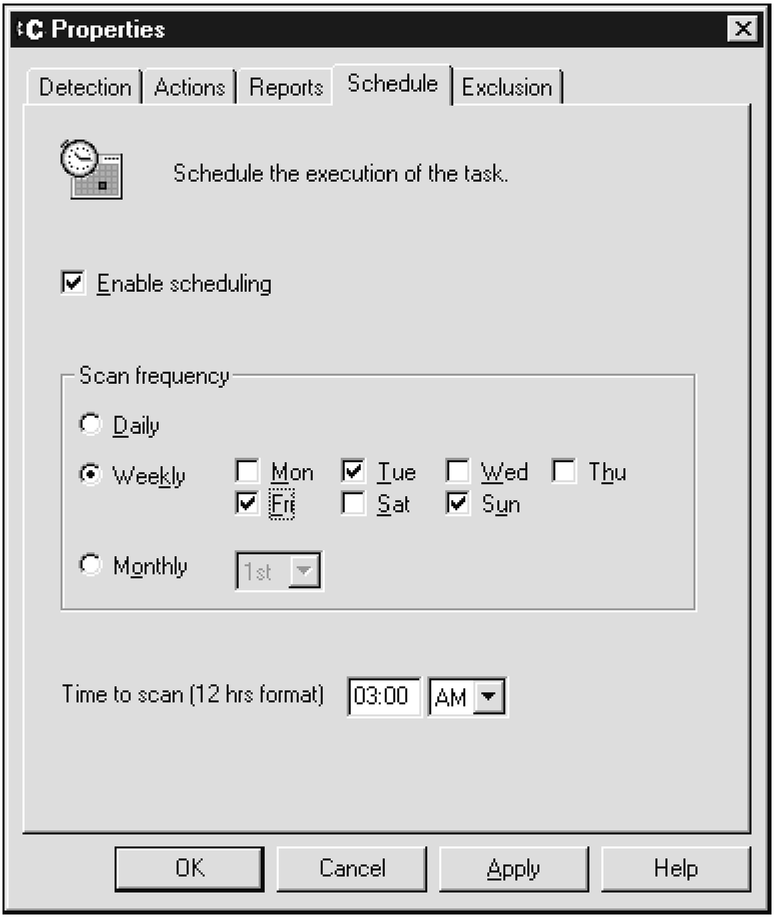
Scheduling Scans

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 the execution of the task.

☑ Enable scheduling

Scan frequency

○ Daily

● Weekly ☐ Mon ☑ Tue ☐ Wed ☐ Thu ☑ Fri ☐ Sat ☑ Sun

○ Monthly 1st

Time to scan (12 hrs format) 03:00 AM

Schedule Dialog Box

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.

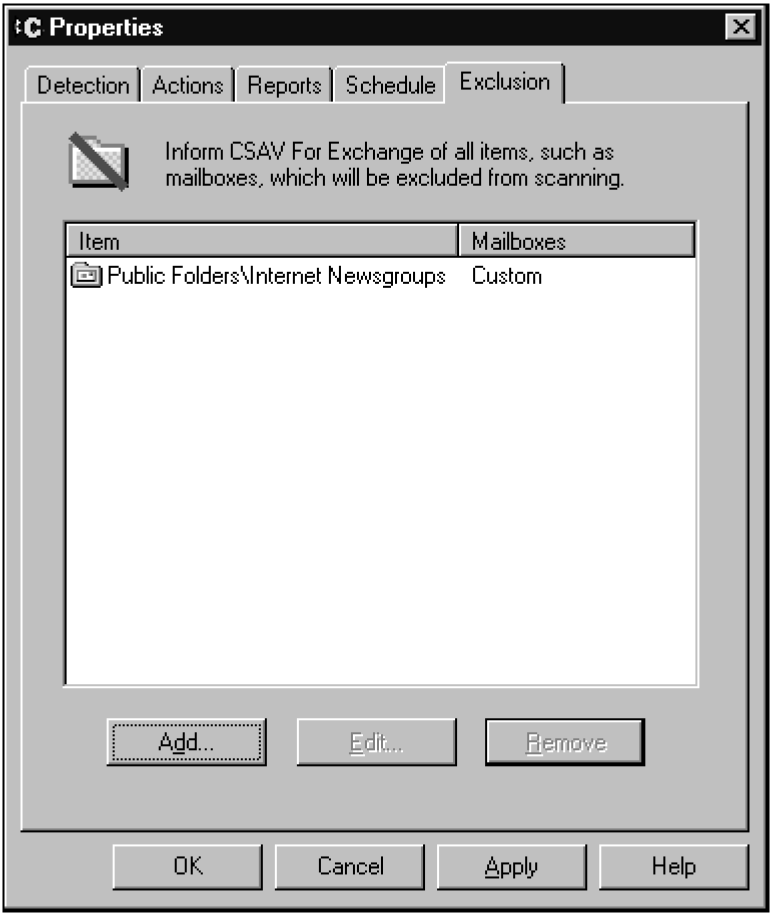
Excluding Specific Items from Scans

The **Exclusion** dialog box allows you to specify which items to exclude from on-demand virus scans. For example, with an on-demand scan, you can exclude the **Outbox** and **Sent Items** folder 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 certain items from an on-demand scan task:

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:



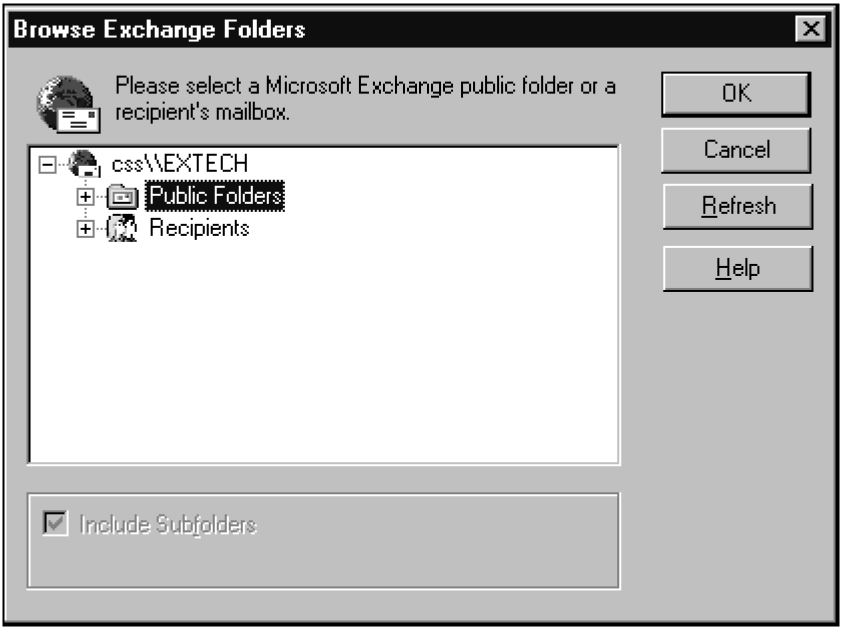
Inform CSAV For Exchange of all items, such as mailboxes, which will be excluded from scanning.

Item	Mailboxes
Public Folders\Internet Newsgroups	Custom

Exclusion Dialog Box (On-demand)

5. 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.

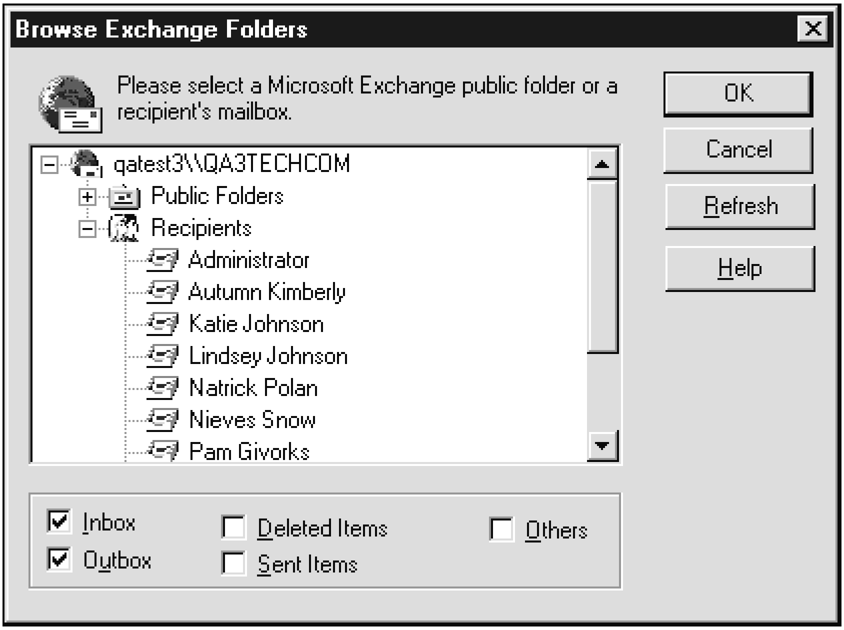


Browse Exchange Folders

Please select a Microsoft Exchange public folder or a recipient's mailbox.

Browse Exchange Folders Dialog Box

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



Browse Exchange Folders

Please select a Microsoft Exchange public folder or a recipient's mailbox.

- qatest3\\QA3TECHCOM
  - Public Folders
  - Recipients
    - Administrator
    - Autumn Kimberly
    - Katie Johnson
    - Lindsey Johnson
    - Natrick Polan
    - Nieves Snow
    - Pam Givorks

☑ Inbox
☑ Outbox
□ Deleted Items
□ Sent Items
□ Others

Browse Exchange Folders Dialog 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** – you can also choose to exclude subfolders. To exclude subfolders select the **Include Subfolders** check box.

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

- If you select a mailbox – the mail item check boxes (**Inbox**, **Outbox**, **Deleted Items**, **Sent Items**, and **Others**) are available for each mailbox. This feature allows you to select different items for each mailbox. Select the mail items that you want to exclude from the scan.

NOTE: If you select multiple single files and/or folders or a block of files and/or folders, the mail item check boxes are only available for the total selection. The mail item check boxes that you select apply to **all** of the files and/or folders that you selected.

NOTE: If you want to exclude all folders, select **Public Folders**. To exclude all recipients, select **Recipients**.

7. Click **OK** to save your modifications.

You can repeat the process for other folders or mailboxes.

VIEWING SCAN STATISTICS

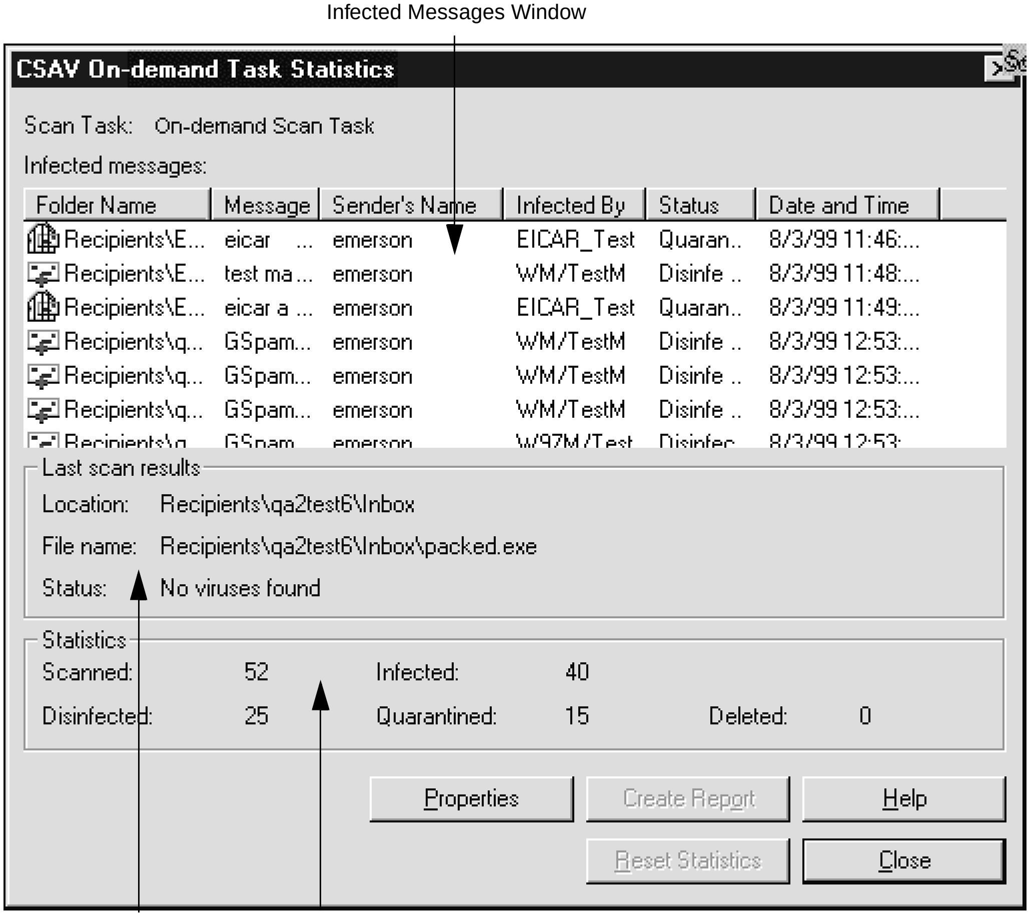
The **Statistics** menu item allows you to view the results of a scan.

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:



CSAV On-demand Task Statistics

Scan Task: On-demand Scan Task

Infected messages:

Folder Name	Message	Sender's Name	Infected By	Status	Date and Time
Recipients\E...	eicar ...	emerson	EICAR_Test	Quaran..	8/3/99 11:46:...
Recipients\E...	test ma ...	emerson	WM/TestM	Disinfe ..	8/3/99 11:48:...
Recipients\E...	eicar a ...	emerson	EICAR_Test	Quaran..	8/3/99 11:49:...
Recipients\q...	GSpam...	emerson	WM/TestM	Disinfe ..	8/3/99 12:53:...
Recipients\q...	GSpam...	emerson	WM/TestM	Disinfe ..	8/3/99 12:53:...
Recipients\q...	GSpam...	emerson	WM/TestM	Disinfe ..	8/3/99 12:53:...
Recipients\q...	GSpam...	emerson	W97M/Test	Disinfec...	8/3/99 12:53:...

Last scan results

Location: Recipients\qa2test6\Inbox

File name: Recipients\qa2test6\Inbox\packed.exe

Status: No viruses found

Statistics

Scanned:	52	Infected:	40		
Disinfected:	25	Quarantined:	15	Deleted:	0

Task Statistics Dialog Box (On-demand)

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, 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** 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.

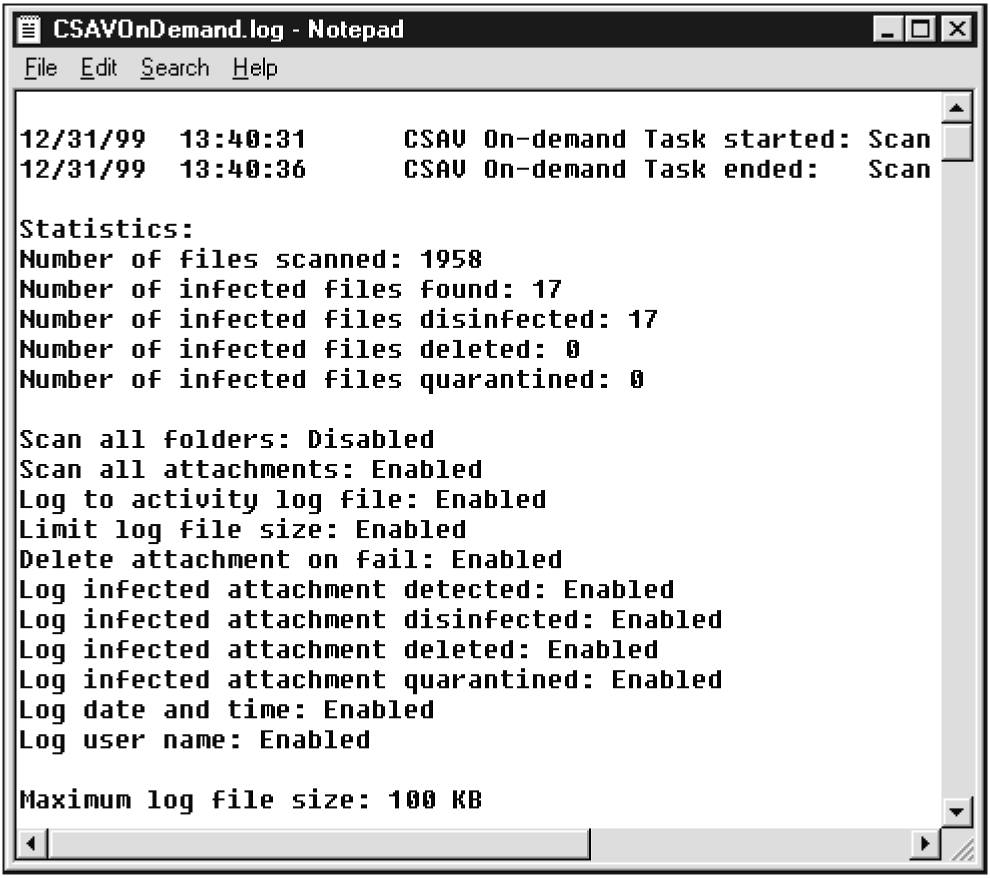
You can save the information in the **Statistics** dialog box to a text file by clicking the **Create Report** button. The system displays the **Save As** dialog box. Name the file and save it.

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:



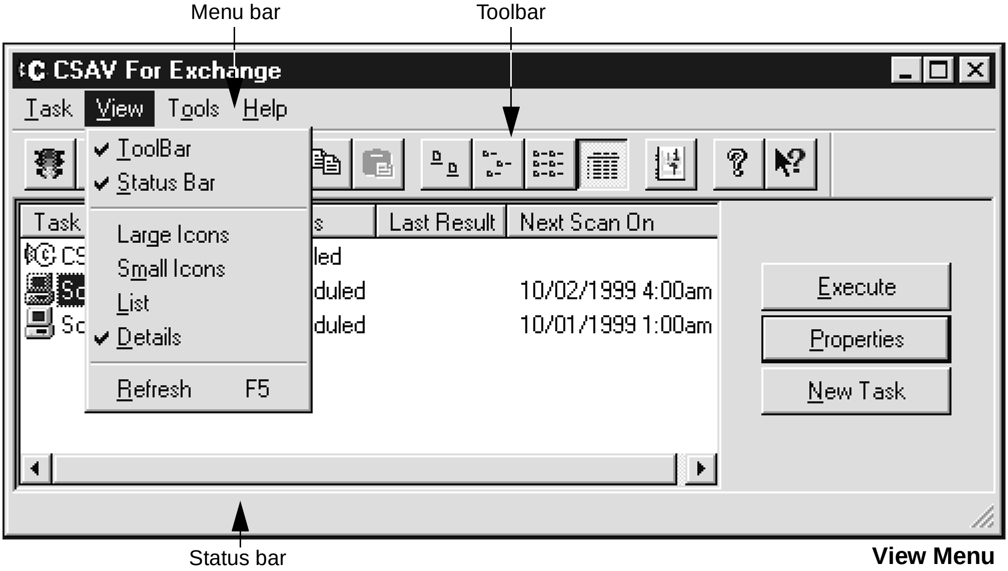
```
12/31/99  13:40:31      CSAV On-demand Task started: Scan
12/31/99  13:40:36      CSAV On-demand Task ended:   Scan

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, see **Reporting** in **Configuring Scanning Properties** located previously in this chapter.

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.



View Menu

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 appearing below 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. Three column headers, **Task Name**, **Last Results**, and **Next Scan On** also display.

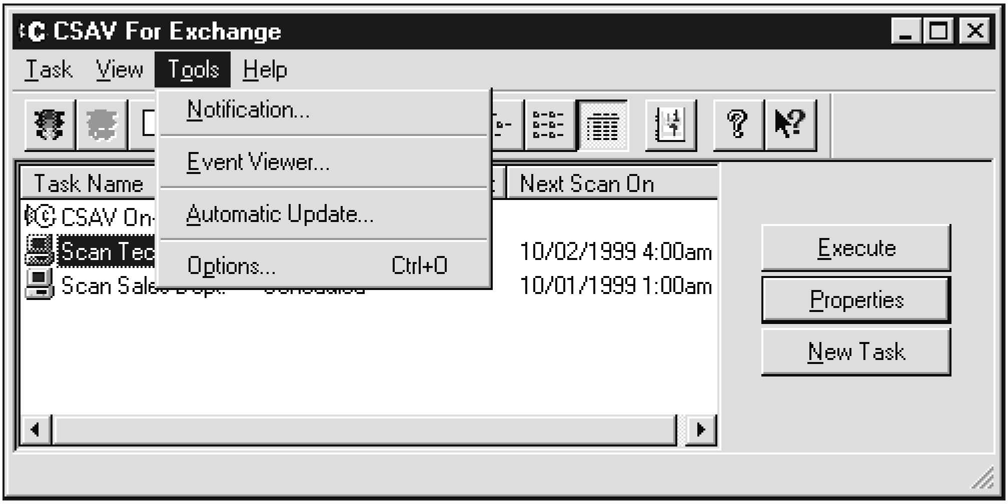
REFRESH

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: **Notification**, **Event Viewer**, **Automatic Update**, and **Options**.

- **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** – Displays the major CSAV for Exchange operations.



Tools Menu

- **Automatic Update** – Allows CSAV to update itself automatically with the latest program files and virus definitions. For more information, see 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 MAPI 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.

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 mail administrator designated at the time of the CSAV for Exchange installation.

You can send a mail alert message to additional administrators, and you can change the text of the message that is 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, see **Options** located later in this chapter.

Although you can cancel sending an alert to the additional administrators that you select, you **cannot** cancel sending an alert to the Microsoft Exchange Server Administrator.

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**.

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 Microsoft Exchange Server Administrator and any other additional administrators that have been specified.

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

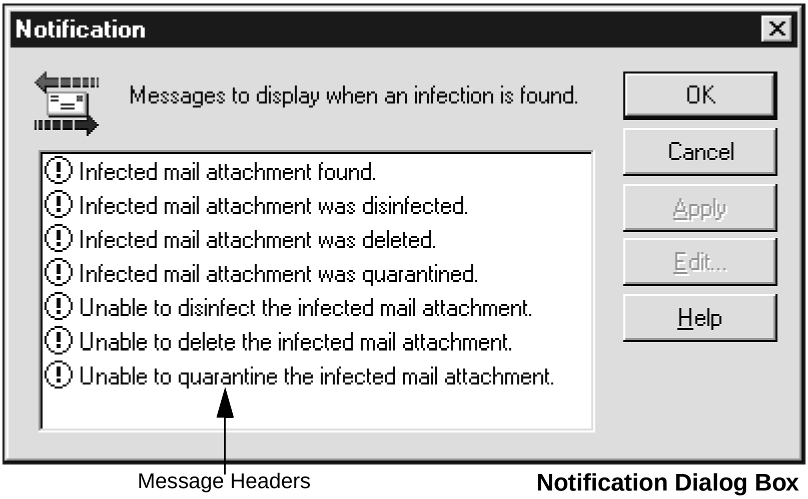
Customizing Virus Notifications

Customizing virus notifications consists of:

- Selecting a message header.
- Specifying additional administrators who will receive **mail alert messages** when a virus is detected through an on-access scan.
- 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:



Messages to display when an infection is found.

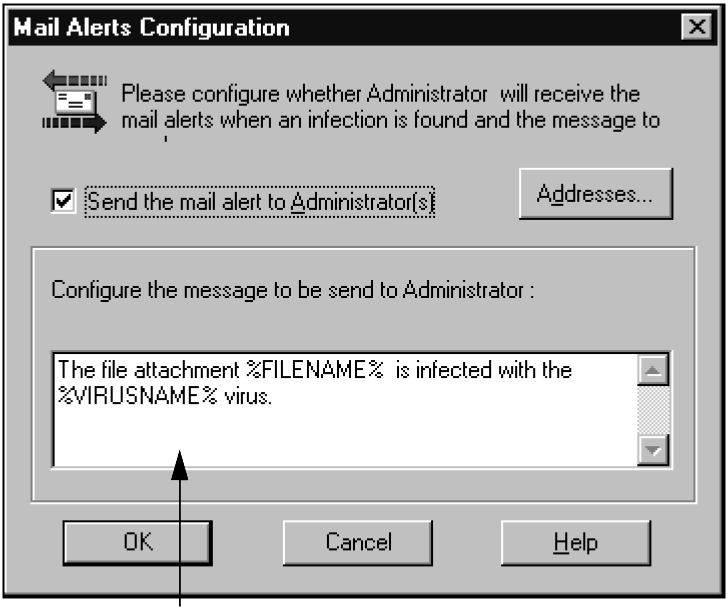
- Infected mail attachment found.
- Infected mail attachment was disinfected.
- Infected mail attachment was deleted.
- Infected mail attachment was quarantined.
- Unable to disinfect the infected mail attachment.
- Unable to delete the infected mail attachment.
- Unable to quarantine the infected mail attachment.

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:



Please configure whether Administrator will receive the mail alerts when an infection is found and the message to

☑ Send the mail alert to Administrator(s)

Configure the message to be send to Administrator :

The file attachment %FILENAME% is infected with the %VIRUSNAME% virus.

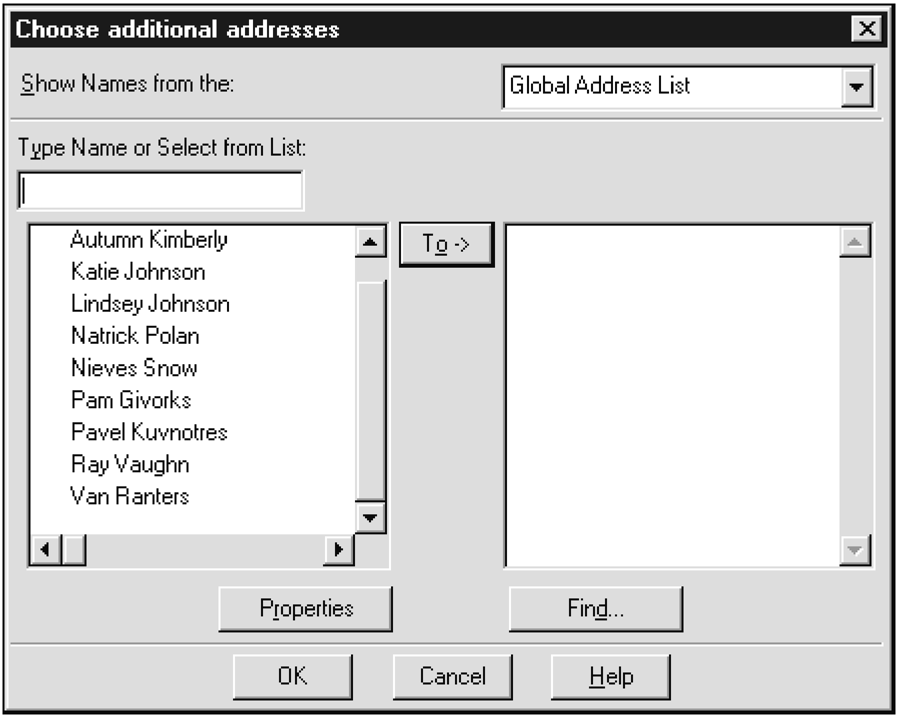
Mail Alert Message Text Box **Mail Alerts Configuration Dialog Box**

6. To send a mail alert message to additional administrators select the **Send the mail alert to Administrator(s)** check box. When you select this option, the **Addresses** button becomes available. This option is selected by default.

NOTE: This option does not change the Microsoft Exchange Server Administrator that you specified during the installation. Although you can cancel sending an alert to the additional administrators that you select, you **cannot** cancel sending an alert to the Microsoft Exchange Server Administrator.

NOTE: Click the option to deselect it. If you deselect **this** option, the message header in the **Notification** dialog box displays an **X** over its icon.

7. Click the **Addresses** button. The system displays the **Choose additional addresses** dialog box:



Choose additional addresses

Show Names from the: Global Address List

Type Name or Select from List:

Autumn Kimberly
Katie Johnson
Lindsey Johnson
Natrick Polan
Nieves Snow
Pam Givorks
Pavel Kuvnotres
Ray Vaughn
Van Ranters

Choosing Additional Addresses Dialog Box

8. Select the administrators from the list and click **OK**. The system returns to the **Mail Alerts Configuration** dialog box.

The **Choose additional addresses** dialog box can contain the names of persons who are **not** administrators. Use caution when selecting names from this dialog box.

9. To modify the default **mail alert message**, edit the text under **Configure the message to be sent to Administrator**.

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, see **Mail Alert Variables** in the ***Appendix***.

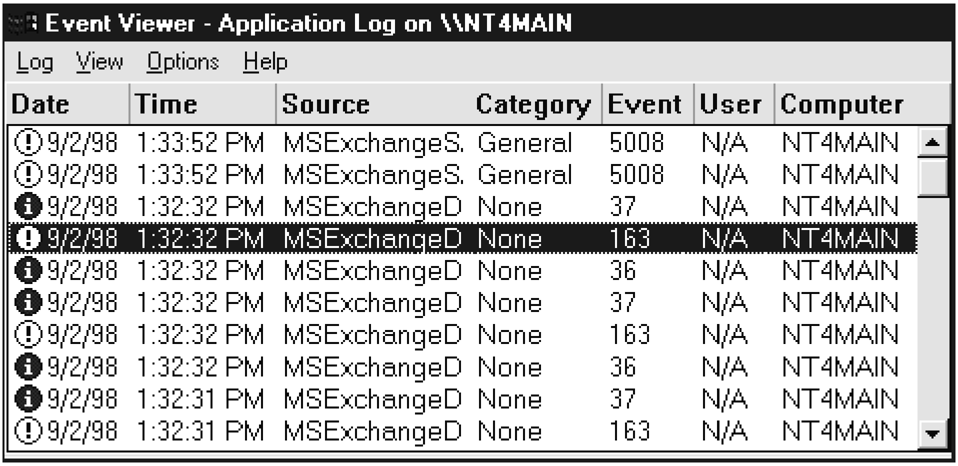
10. Click **OK** to save your changes.

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

USING EVENT VIEWER

In Windows NT's **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. In **Event Viewer**, click **Log** on the menu bar. Then, click the **Application** menu item. The system displays a log of application-related events:

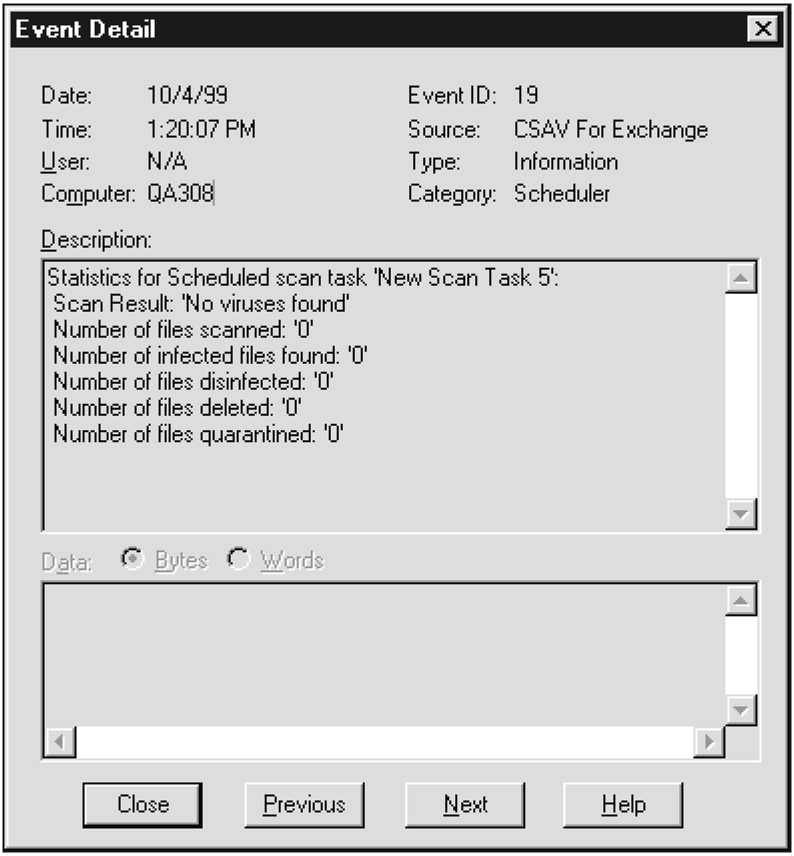


Date	Time	Source	Category	Event	User	Computer
! 9/2/98	1:33:52 PM	MSExchangeS.	General	5008	N/A	NT4MAIN
! 9/2/98	1:33:52 PM	MSExchangeS.	General	5008	N/A	NT4MAIN
i 9/2/98	1:32:32 PM	MSExchangeD	None	37	N/A	NT4MAIN
! 9/2/98	1:32:32 PM	MSExchangeD	None	163	N/A	NT4MAIN
i 9/2/98	1:32:32 PM	MSExchangeD	None	36	N/A	NT4MAIN
i 9/2/98	1:32:32 PM	MSExchangeD	None	37	N/A	NT4MAIN
! 9/2/98	1:32:32 PM	MSExchangeD	None	163	N/A	NT4MAIN
i 9/2/98	1:32:32 PM	MSExchangeD	None	36	N/A	NT4MAIN
i 9/2/98	1:32:31 PM	MSExchangeD	None	37	N/A	NT4MAIN
! 9/2/98	1:32:31 PM	MSExchangeD	None	163	N/A	NT4MAIN

Event Viewer Application Log

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 Detail** box with information on the event:



Event Detail

Date: 10/4/99
Time: 1:20:07 PM
User: N/A
Computer: QA308
Event ID: 19
Source: CSAV For Exchange
Type: Information
Category: Scheduler

Description:

```
Statistics for Scheduled scan task 'New Scan Task 5':
 Scan Result: 'No viruses found'
 Number of files scanned: '0'
 Number of infected files found: '0'
 Number of files disinfected: '0'
 Number of files deleted: '0'
 Number of files quarantined: '0'
```

Data: ● Bytes ○ Words

Event Detail Box

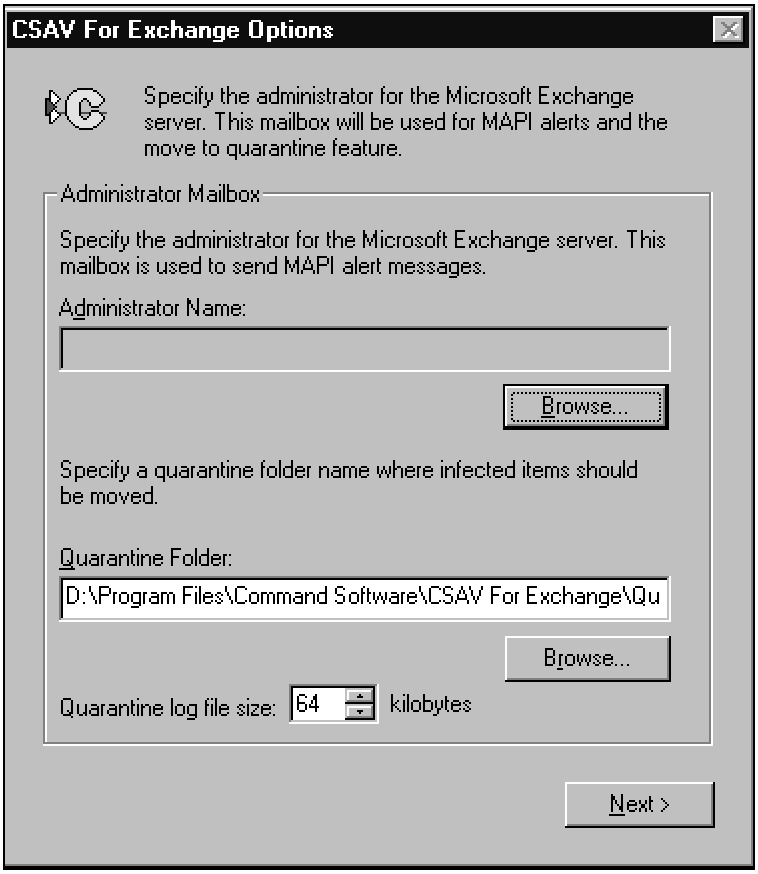
OPTIONS

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 MAPI 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.

NOTE: You can configure CSAV for Exchange to send virus notifications to more than one administrator. For more information, see **Configuring Virus Notifications** located previously in this chapter.

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

Specify the administrator for the Microsoft Exchange server. This mailbox will be used for MAPI alerts and the move to quarantine feature.

Administrator Mailbox

Specify the administrator for the Microsoft Exchange server. This mailbox is used to send MAPI alert messages.

Administrator Name:

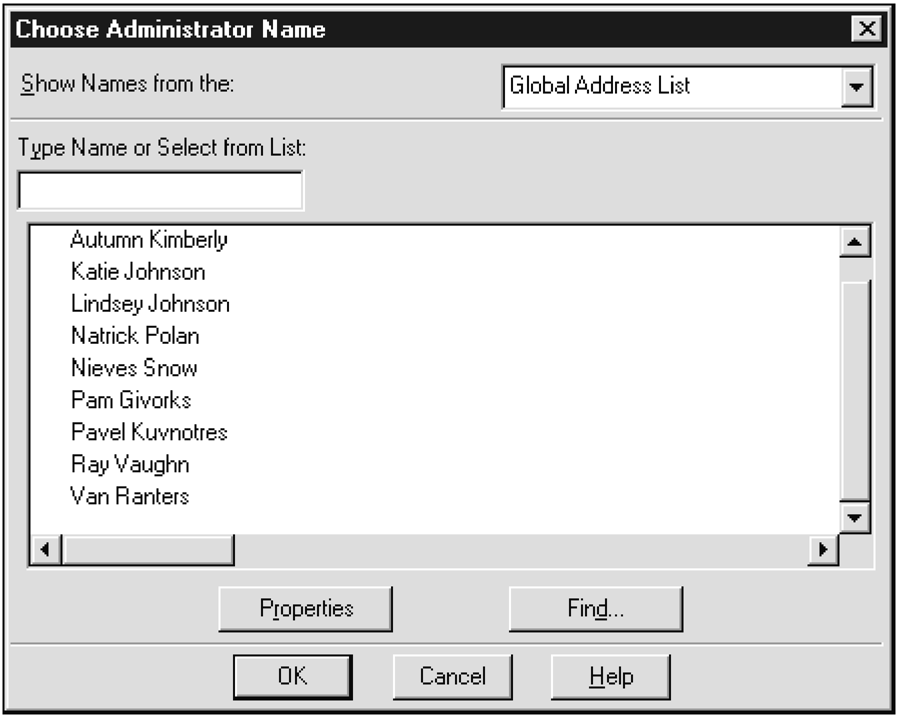
Specify a quarantine folder name where infected items should be moved.

Quarantine Folder: D:\Program Files\Command Software\CSAV For Exchange\Qu

Quarantine log file size: 64 kilobytes

CSAV for Exchange Options Dialog Box

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

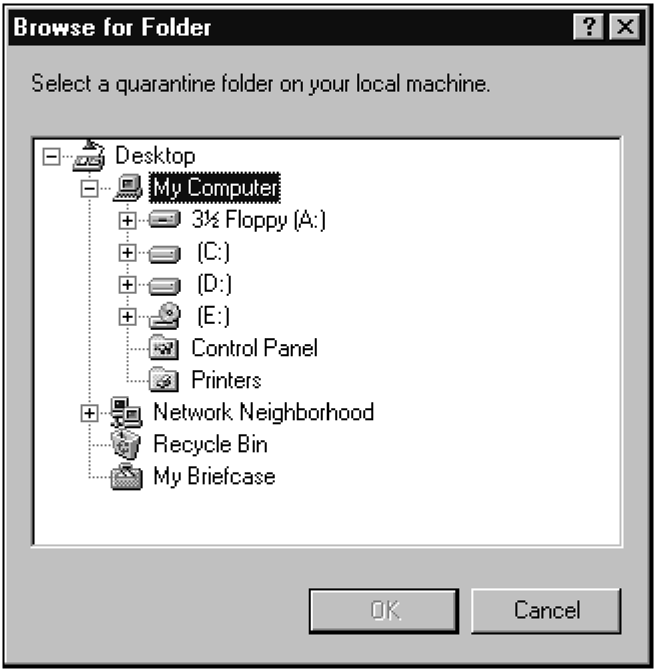


Show Names from the: Global Address List

Autumn Kimberly
Katie Johnson
Lindsey Johnson
Natrick Polan
Nieves Snow
Pam Givorks
Pavel Kuvnotres
Ray Vaughn
Van Ranters

Choose Administrator Name Dialog Box

4. Select an administrator from the list of available names.
5. Click **OK**. The system redisplays the **CSAV for Exchange Options** dialog box.
6. 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

Select a quarantine folder on your local machine.

Browse for Folder Dialog Box

7. Select a quarantine folder from the list of available folders.
8. Click **OK**. The system redisplays the **CSAV for Exchange Options** dialog box.
9. In the **Quarantine log file size** box, specify the size you want for the quarantine log file. The default is **64 KB**. The minimum size is **10 KB** and the maximum is **999 KB**.

NOTE: The existing quarantine log file is overwritten when the amount of data within it exceeds the limit you have specified in the **Quarantine log file size** box.

10. Click **OK**.

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.

ABOUT CSAV FOR EXCHANGE

This menu item displays the product's version number and copyright 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 extension with **.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.

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 dialog box consists of the **Update** dialog box and the **Schedule** dialog box.

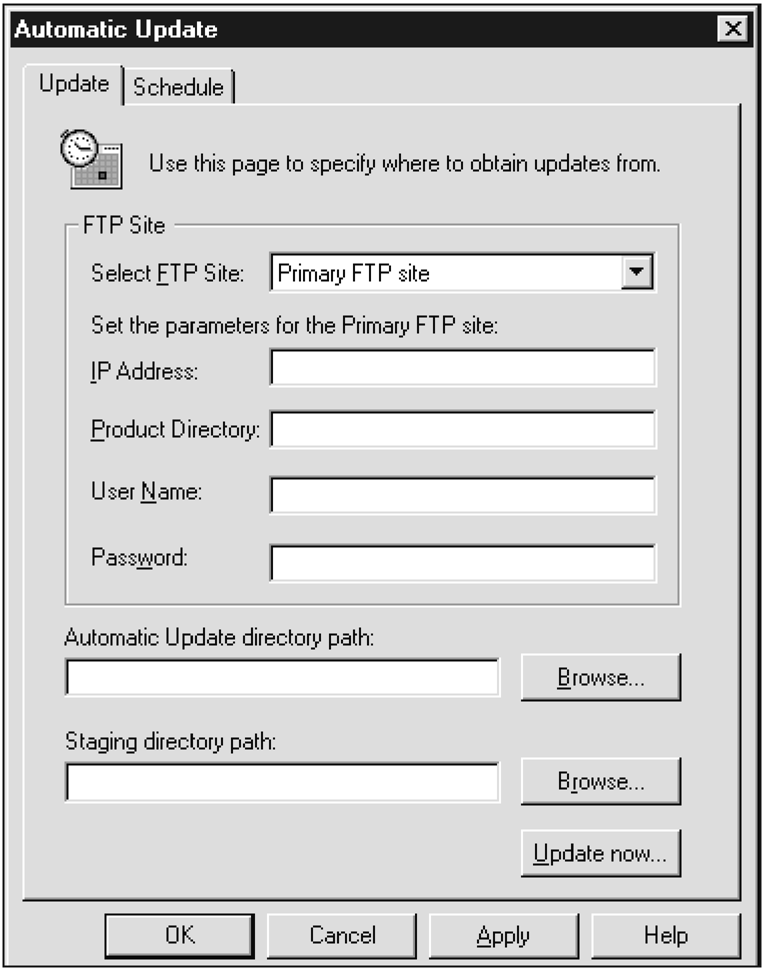
The **Update** dialog box is divided into two sections. The upper section contains the **FTP Site** group box. The lower section contains text boxes for the **Automatic Update directory path** and the **Staging directory path**.

By default, the **FTP Site** group box contains primary and secondary FTP site IP addresses and product directories. It is from these sites that CSAV for Exchange downloads its update files. You can change the primary and secondary FTP site IP addresses if necessary.

If you decide to use non-default FTP site IP addresses, be sure to provide the correct paths to the CSAV for Exchange product directories at those addresses.

To open the **Automatic Update** dialog box, click **Tools** on the menu bar and then click **Automatic Update**. The system displays the **Automatic Update** dialog box with the **Update** dialog box in view.

AUTOMATIC UPDATE



Automatic Update

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:

Product Directory:

User Name:

Password:

Automatic Update directory path:

Staging directory path:

Update Dialog Box

Clicking the down arrow on the **Select FTP Site** text box allows you 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**

To complete the required information, follow these steps:

1. Click the drop-down arrow in the **Select FTP Site** text box.
2. Select **Primary FTP site** from the drop-down list.
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 in the IP address for the FTP site.

4. In the **Product Directory** text box, type in 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 **Steps 1** through **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. Type the path to the **automatic update directory** in the **Automatic Update directory path** text box. 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.

NOTE: You are not required to type anything into the **Staging directory path** text box. By default, this text box is blank. CSAV for Exchange uses the Windows temporary directory as the **staging directory**.

9. 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

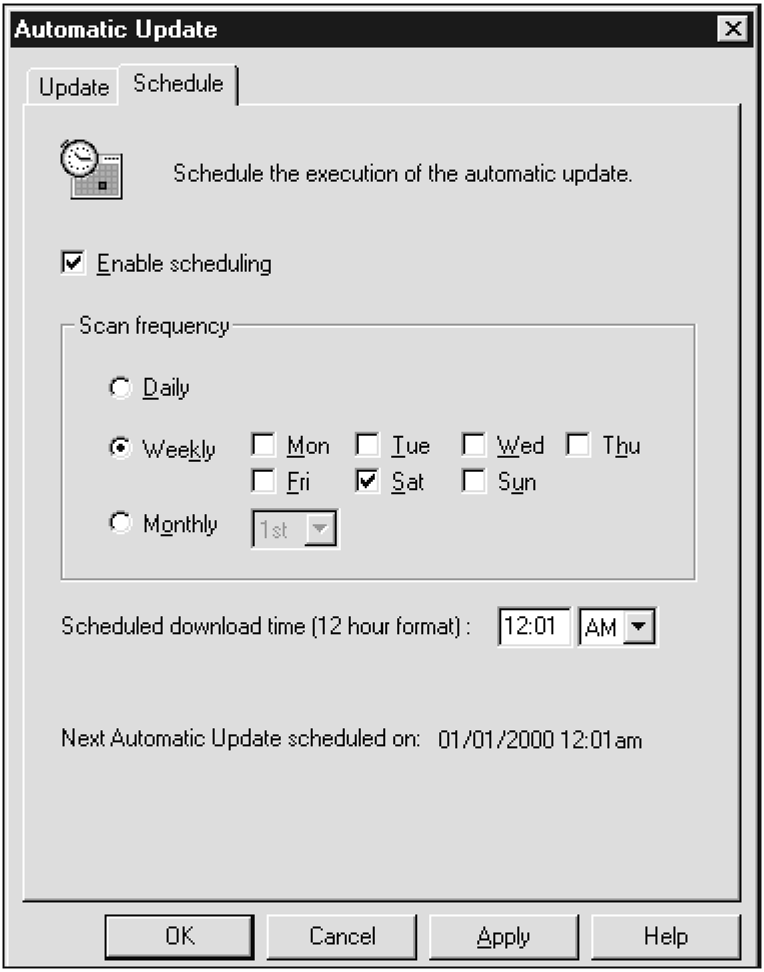
After you have entered all of the necessary information in the **Update** dialog box, you can perform an on-demand update of CSAV for Exchange. To perform the update, click the **Update now** button. CSAV for Exchange downloads the latest update files and then immediately updates your system.

Scheduled Updates

You can configure CSAV for Exchange to download update files automatically according to a schedule that you determine. 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.



Schedule the execution of the automatic update.

☑ Enable scheduling

Scan frequency

○ Daily

● Weekly ☐ Mon ☐ Tue ☐ Wed ☐ Thu
☐ Fri ☑ Sat ☐ Sun

○ Monthly 1st

Scheduled download time (12 hour format) : 12:01 AM

Next Automatic Update scheduled on: 01/01/2000 12:01am

Schedule Dialog Box

2. Select the **Enable Scheduling** option.
3. Select **Daily**, **Monthly** or **Weekly**. If you select **Weekly**, select the days on which you would like the scheduled downloads to occur. If you select **Monthly**, click the drop-down arrow to specify the day of the month you want the download to take place.

4. Using the **00:00** format, type a time in the **Scheduled download time (12 hour format)** text box. Then, use the drop-down arrow to select **AM** or **PM**.
5. Click **OK** to save your changes.

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

5

GLOSSARY

BOOT SECTOR

Stores critical drive information. Floppy disks and local hard disks have boot sectors.

BOOT SECTOR VIRUS

A virus that infects the boot sector of a hard disk or a floppy disk. Note that any formatted disk (even one that is blank or contains only text data) can contain a boot sector virus. Booting with an infected disk activates this type of virus.

CIRCULAR INFECTION

A type of infection that occurs when two viruses infect the boot sector of a disk, rendering the disk unbootable. Removing one virus usually causes a re-infection with the other virus.

CMOS

Complimentary Metal Oxide Semi-Conductor. CMOS stores critical configuration information. Some viruses try to alter this data.

COMPANION VIRUS

A virus that infects executable files by creating a companion file with the same name but with a .COM extension. As DOS executes .COM files before .EXE files and .BAT files, the virus loads before the executable file.

CROSS-LINKED FILES

Cross-linking, a common situation rarely associated with viruses, occurs when two files seem to share the same clusters on the disk.

DROPPER

A program compressed with PKLite, Diet, LZExe, etc... that contains a virus. Microsoft Word documents can also function as droppers. A dropper deposits the virus onto a hard disk, a floppy disk, a file or into memory. The children of this process are not droppers.

EICAR TEST FILE

EICAR (European Institute for Antivirus Research) test file provides an industry standard solution to test anti-virus products. The EICAR test file is the result of a cooperative effort between various anti-virus researchers. You can use this file in a variety of ways. For example, you can safely verify that real-time protection is active and demonstrate what happens when it finds a virus.

ENCRYPTION

A process of making data unreadable. Some viruses use encryption techniques in order to hide their presence from anti-virus scanners.

EXECUTABLE CODE

Instructions that a computer uses to accomplish various tasks. This includes COM, EXE, DLL and similar files. In a broader sense, executable code includes the code found in disk boot sectors, batch files and even macros used by some applications.

FALSE POSITIVE

A false positive occurs when a scanner identifies a file as infected when, in fact, the file is virus-free.

FILE STEALTH

A virus characteristic that hides the increase in length of infected files. For example, if the original size of a file is 240 KB, the file would appear to remain the same size although the file now contains a virus.

FULL STEALTH

A virus that tries to hide its presence on an infected system. When operational, a full stealth virus can evade attempts to search for it in files or memory.

HEURISTICS

A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures.

The advantage of the heuristics scan is that new variants of existing viruses cannot fool it. However, heuristics scans occasionally report suspicious code in normal programs. For example, the scanning of a program may generate the following message:

```
C:\DOS\MSHERC.COM has been modified by adding some code
at the end. This does not appear to be a virus, but
might be a self-checking routine or some "wrapper"
program.
```

Command AntiVirus issues a stronger warning based on the likelihood of a program actually containing a virus.

INTEGRITY CHECKER

A program that checks for changes to files. Integrity checkers, when used correctly, can provide an excellent second line of defense against new viruses or variants.

JOKE PROGRAMS

A program that makes the computer behave oddly. Command AntiVirus detects the presence of several well-known joke programs. While joke programs are generally harmless, their side effects are often mistaken for those of a virus.

LOGIC BOMB

A program that runs a pre-programmed routine (frequently destructive) when a designated condition is met. Logic bombs do not make copies of themselves.

MALWARE

A generic name for software that intentionally performs actions that can damage data or disrupt systems.

MACRO VIRUS

A virus written in one of the many macro languages. The macro viruses spread via infected files such as documents, spreadsheets, databases, or any computer program that uses a macro languages.

MASTER BOOT RECORD (MBR)

The first physical sector on all PC hard disks reserved for a short bootstrap program. The MBR also contains the partition table.

MEMORY-RESIDENT

Residing in computer memory as opposed to on the disk.

MULTIPARTITE

A virus that is able to infect both files and boot sectors. Such viruses are highly infectious.

ON-ACCESS SCAN

A virus scan that starts when the operating system performs an action on a file. For instance, when a file is created on the hard disk, Command AntiVirus' on-access protection scans it immediately. If a virus is detected, CSAV performs the action you specified in the on-access scan task settings.

ON-DEMAND SCAN

A virus scan that is started manually. In CSAV, on-demand scans can also be configured to scan automatically at a specified time (see the glossary entry for **Scheduled Scan**).

PARTITION TABLE

A place on a hard disk containing information required to access the partitions (logical blocks) of a PC disk. The partition table also contains a flag indicating which partition should be used to boot the system (the active partition). The partition table is stored in the master boot record (MBR).

POLYMORPHISM

A virus in which the code appears to be different every time the virus reproduces (though generally each reproduction of the virus is functionally identical). This process is usually achieved by encrypting the body of the virus and adding a decryption routine that is different for each reproduction.

SCHEDULED SCAN

An on-demand scan that is configured to run automatically each day, once a day on specified days of the week, or once a month on a given date.

STEALTH VIRUS

A virus that tries to hide itself. Changes made by this virus are not easily detected. For example, if the original size of a file is 240K, the infected file would appear to remain the same size. A stealth virus can operate only when it is resident in memory.

TROJAN (OR TROJAN HORSE)

A program that carries out an unauthorized function while hidden inside an authorized program. This program is designed to do something other than what it claims to and frequently is destructive in its actions.

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 (see the glossary entry for **Companion Viruses***).* It may attach itself to any executable code, including but not limited to boot sectors and/or partition sectors of hard and/or floppy disks. It may damage, corrupt or destroy data, or degrade system performance.

VIRUS SIMULATOR

A program that creates files that “look like” viruses. Such files are useless for testing purposes because they are not really infected. Command AntiVirus is smart enough not to be fooled by a simulator.

VIRUS VARIANT

A modification of a previously known virus, a variation.

WORM

A program that reproduces by copying itself over and over, system to system. Worms are self-contained and generally use networks to spread.

APPENDIX

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 – 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 – About CSAV for Exchange	Alt + H and A

MAIL ALERT VARIABLES

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

```
The message you sent to %RECIPIENT% has the file
attachment %FILENAME% that was infected with the
%VIRUSNAME% virus.
```

When a virus is detected, the variables in the message are replaced by values. In the previous example, the values consist of the e-mail’s intended recipients (%RECIPIENTS%), the name of the infected e-mail attachment (%FILENAME%), and the name of the virus infecting the attachment (%VIRUSNAME%). Thus, the mail alert message received by the sender of the infected e-mail would look something like:

```
The message you sent to John Public has the file
attachment program.zip that was infected with the
Sylvia virus.
```

CSAV for Exchange uses five different variables. These variables are:

- %COMPUTERNAME% – the name of the CSAV for Exchange computer where the infection was found
- %FILENAME% – the name of the infected e-mail attachment
- %RECIPIENT% – the names of the intended e-mail recipients
- %SENDER% – the name of the e-mail sender
- %VIRUSNAME% – the name of the virus infecting the e-mail attachment

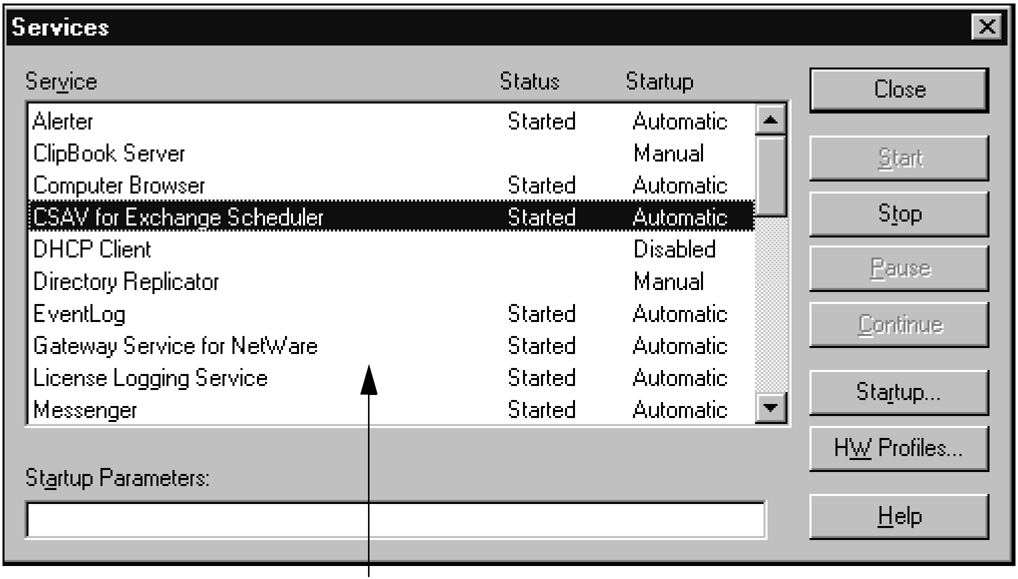
CSAV SERVICE STARTUP OPTIONS

Command AntiVirus for Exchange runs the **CSAV for Exchange Scheduler** service. Through the **Windows NT 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 Windows NT Server starts.

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 NT taskbar, click the **Start** button.
2. Select **Settings**.
3. Click **Control Panel**.
4. Double-click the **Services** icon. The system displays the **Services** dialog box:



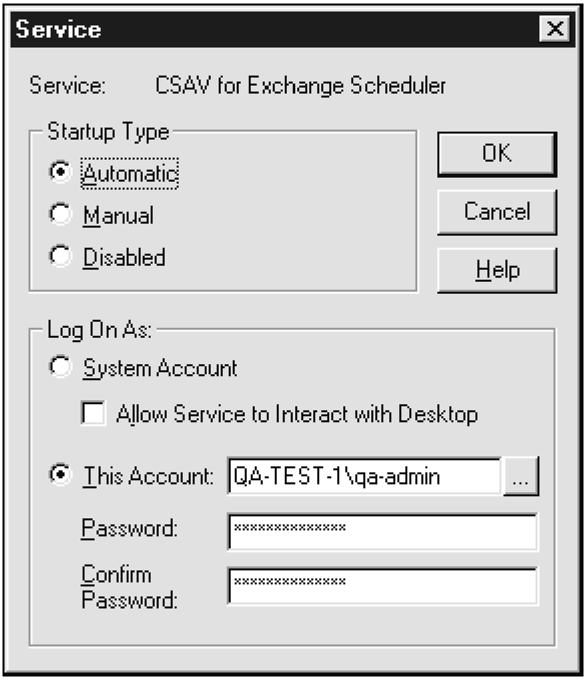
Service	Status	Startup
Alerter	Started	Automatic
ClipBook Server		Manual
Computer Browser	Started	Automatic
CSAV for Exchange Scheduler	Started	Automatic
DHCP Client		Disabled
Directory Replicator		Manual
EventLog	Started	Automatic
Gateway Service for NetWare	Started	Automatic
License Logging Service	Started	Automatic
Messenger	Started	Automatic

Startup Parameters:

Services Window

Services Dialog Box

5. In the **Services** window, select the **CSAV for Exchange Scheduler** service.
6. Click the **Startup** button. The system displays the **Service** dialog box:



Service

Service: CSAV for Exchange Scheduler

Startup Type

● Automatic

○ Manual

○ Disabled

Log On As:

○ System Account

□ Allow Service to Interact with Desktop

● This Account: QA-TEST-1\qa-admin

Password: ***************

Confirm Password: ***************

Service Dialog Box

7. In the **Service** dialog box, select which **Startup Type** you prefer: **Automatic**, **Manual**, or **Disabled**. **Automatic** is the default setting. If you select **Manual**, the **CSAV for Exchange Schedule**r service that you selected in **Step 5** starts only if you launch it manually after Windows NT starts. If you select **Disable**, the service starts again only if you reset the service to **Manual** or **Automatic**.
8. To finish, click **OK**.

INDEX