

**Command Interceptor™**

**for**

**MIMESweeper™**

**Administrator's Guide**



# NOTICE

---

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

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

## LICENSE AGREEMENT

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

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

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

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

## WARRANTY

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

**Command AntiVirus © Copyright 2002 by Command Software Systems, Inc.  
Portions © Copyright 1993, 2002 FRISK Software International.**

**Published in the U.S.A. by Command Software Systems, Inc. All rights reserved.  
Document No. CIM-4X-0902**

**Part No. 07-7000-01**

# TABLE OF CONTENTS

|  |            |
|--|------------|
| <b>INTRODUCTION .....</b>  | <b>1-1</b> |
| Main Features .....  | 1-1        |
| Chapter Overview .....   | 1-2        |
| Chapter 1 - Introduction .....                                   | 1-2        |
| Chapter 2 - CS MAILsweeper 4.3 for SMTP .....                    | 1-2        |
| Chapter 3 - MAILsweeper 4.2 for SMTP .....                       | 1-2        |
| Chapter 4 - MAILsweeper 4.1 .....                                | 1-2        |
| Chapter 5 - MAILsweeper 4.0 .....                                | 1-3        |
| Chapter 6 - MAILsweeper 3.2 .....                                | 1-3        |
| Chapter 7 - WEBSweeper 4.0 .....                                 | 1-3        |
| Conventions Used .....   | 1-4        |
| Additional Information .....                                     | 1-5        |
| Web Site .....   | 1-5        |
| Mailing List Server .....  | 1-5        |
| <b>CS MAILSWEEPER 4.3 FOR SMTP .....</b>                         | <b>2-1</b> |
| Pre-installation Requirements .....                              | 2-1        |
| Installing the Command Interceptor Scenario .....                | 2-2        |
| Installing Command Interceptor .....                             | 2-9        |
| Installing Command Interceptor for MIMESweeper .....             | 2-10       |
| Creating a Stripped Classification .....                         | 2-12       |
| Creating and Enabling the Command Interceptor Scenario .....     | 2-17       |
| Scheduling Command Interceptor Definition File Updates .....     | 2-28       |
| Updating the Command Interceptor Definition Files Manually ..... | 2-37       |
| Changing Your Command Interceptor For MIMESweeper Password ..... | 2-38       |
| Removing Command Interceptor for MIMESweeper .....               | 2-39       |
| Removing An Anti-virus Scenario .....                            | 2-41       |
| <b>MAILSWEEPER 4.2 FOR SMTP .....</b>                            | <b>3-1</b> |
| Pre-installation Requirements .....                              | 3-1        |
| Installing .....   | 3-2        |
| Installing the Command AntiVirus Scenario .....                  | 3-2        |
| Installing Command Interceptor for MIMESweeper .....             | 3-3        |
| Scheduling Command Interceptor Definition File Updates .....     | 3-6        |
| Enabling the Command AntiVirus Scenario .....                    | 3-15       |
| Creating a Delete Classification .....                           | 3-17       |
| Updating the Command Interceptor Definition Files Manually ..... | 3-18       |
| Changing Your Command Interceptor For MIMESweeper Password ..... | 3-19       |
| Removing Command Interceptor for MIMESweeper .....               | 3-20       |

---

|  |            |
|--|------------|
| <b>MAILSWEEPER 4.1</b> .....                                     | <b>4-1</b> |
| Pre-installation Requirements .....                              | 4-1        |
| Installing .....   | 4-2        |
| Installing Command Interceptor for MIMESweeper .....             | 4-2        |
| Enabling the Command AntiVirus Scenario .....                    | 4-4        |
| Creating a Delete Classification .....                           | 4-6        |
| Updating the Command AntiVirus Definition Files .....            | 4-7        |
| Removing Command Interceptor for MIMESweeper .....               | 4-8        |
| <b>MAILSWEEPER 4.0</b> .....                                     | <b>5-1</b> |
| Pre-installation Requirements .....                              | 5-1        |
| Installing .....   | 5-2        |
| Installing Command Interceptor for MIMESweeper .....             | 5-2        |
| Enabling the Command AntiVirus Scenario .....                    | 5-4        |
| Creating a Delete Classification .....                           | 5-6        |
| Updating the Command AntiVirus Definition Files .....            | 5-7        |
| Removing Command Interceptor for MIMESweeper .....               | 5-8        |
| <b>MAILSWEEPER 3.2</b> .....                                     | <b>6-1</b> |
| Pre-installation Requirements .....                              | 6-1        |
| Installing .....   | 6-2        |
| Removing Command Interceptor for MIMESweeper .....               | 6-4        |
| <b>WEBSWEEPER 4.X</b> .....                                      | <b>7-1</b> |
| Pre-installation Requirements .....                              | 7-1        |
| Installing .....   | 7-2        |
| Installing the Command AntiVirus Scenario .....                  | 7-2        |
| Installing Command Interceptor for MIMESweeper .....             | 7-3        |
| Scheduling Command Interceptor Definition File Updates .....     | 7-5        |
| Enabling the Command AntiVirus Scenario .....                    | 7-14       |
| Creating a Delete Classification .....                           | 7-16       |
| Updating the Command Interceptor Definition Files Manually ..... | 7-17       |
| Changing Your Command Interceptor For MIMESweeper Password ..... | 7-18       |
| Removing Command Interceptor for MIMESweeper .....               | 7-19       |

# INTRODUCTION



Command Interceptor™ for MIMESweeper™ is a plugin for MAILsweeper™ or WEBSweeper™ that provides the latest technology for preventing the spread of computer viruses. This allows you to integrate the most up-to-date anti-virus protection with the security solution that best meets your technical and operational needs.

## MAIN FEATURES

---

The Command Interceptor for MIMESweeper plugin:

- Provides detection and disinfection of viruses in incoming and outgoing e-mail. Command Interceptor for MAILsweeper 3.2 provides only detection.
  - Uses state-of-the-art technology to scan for thousands of known viruses and their variants.
  - Scans for macro viruses and Trojan Horses.
  - Scans compressed files and compressed executables.
  - Removes viruses without damaging the original file.
-

## CHAPTER OVERVIEW

---

The *Command Interceptor for MIMESweeper™ Administrator's Guide* consists of the following chapters:

### CHAPTER 1 - INTRODUCTION

This chapter provides an overview of the product including a list of features and conventions.

### CHAPTER 2 - CS MAILSWEEPER 4.3 FOR SMTP

Chapter 2 provides pre-installation requirements and instructions on how to install the Command Interceptor Scenario and the Command Interceptor for MIMESweeper. This chapter also includes information on scheduling Command AntiVirus definition file updates, creating a Stripped classification, creating and enabling the Command Interceptor Scenario, and removing the Command Interceptor for MIMESweeper.

### CHAPTER 3 - MAILSWEEPER 4.2 FOR SMTP

This chapter provides pre-installation requirements and instructions on how to install the Command AntiVirus Scenario for MAILsweeper and the Command Interceptor for MIMESweeper. Chapter 3 also includes information on scheduling Command AntiVirus definition file updates, creating a Delete classification, enabling the Command AntiVirus Scenario, and removing the Command Interceptor for MIMESweeper.

### CHAPTER 4 - MAILSWEEPER 4.1

Chapter 4 provides pre-installation requirements and instructions on how to install the Command Interceptor for MIMESweeper. This chapter also includes information on creating a Delete classification, enabling the Command AntiVirus Scenario, updating the Command AntiVirus definition files, and removing the Command Interceptor for MIMESweeper.

## CHAPTER 5 - MAILSWEEPER 4.0

This chapter provides pre-installation requirements and instructions on how to install the Command Interceptor for MIMESweeper. Chapter 5 also includes information on creating a delete classification, enabling the Command AntiVirus Scenario, updating the Command AntiVirus definition files, and removing the Command Interceptor for MIMESweeper.

## CHAPTER 6 - MAILSWEEPER 3.2

Chapter 6 provides pre-installation requirements and instructions on how to install and remove the Command Interceptor for MIMESweeper.

## CHAPTER 7 - WEBSWEEPER 4.0

This chapter provides pre-installation requirements and instructions on how to install the Command AntiVirus Scenario for WEBSweeper™ and the Command Interceptor for MIMESweeper™. Chapter 7 also includes information on scheduling Command AntiVirus definition file updates, creating a Delete classification, enabling the Command AntiVirus Scenario, and removing the Command Interceptor for MIMESweeper.

## CONVENTIONS USED

---



Indicates an area that requires special attention.



Indicates a helpful tip.



Indicates network-specific information.

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

```
C:\MSW\PROGRAM
```

**CSAV** The acronym used for Command AntiVirus.

*Italics* A reference to the manual is in italics.

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

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



## ADDITIONAL INFORMATION

---

### WEB SITE

You will find a wealth of fascinating information on the Command Software Systems web site. Do you have questions about viruses? Do you want to know more about security? Would you like to know the answers to our customers' most frequently asked questions? We provide comprehensive information on viruses, products, events, employment opportunities and much more. Plus, for your convenience, all of our readme files, quick start guides, and manuals are available for online viewing.

Be sure to visit this exciting extension of Command Software Systems' services at:

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

### 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.





# CS MAILSWEEPER 4.3 FOR SMTP

To enable Command Interceptor™ protection, you must install the Command Interceptor for MIMESweeper™. The instructions in this chapter can be used to install the Command Interceptor from the downloaded file or from the CD.

## PRE-INSTALLATION REQUIREMENTS

---

Before installing the Command Interceptor for MIMESweeper, your system must:

- Have CS MAILsweeper™ 4.3 for SMTP installed on an NTFS-formatted partition.
- Have the Command Interceptor Scenario installed. For more information, refer to **Installing the Command Interceptor Scenario** located later in this section.
- Not have any e-mail anti-virus program installed.



**NOTE:** To remove a previously installed e-mail anti-virus program, use the **Add/Remove Programs** feature in the Windows 2000/XP Control Panel. For more information, refer to **Removing An Anti-virus Scenario** located later in this chapter.

- Not have any anti-virus real-time protection active.

If your system does not meet the above-mentioned requirements, Command Interceptor may not function correctly.

---

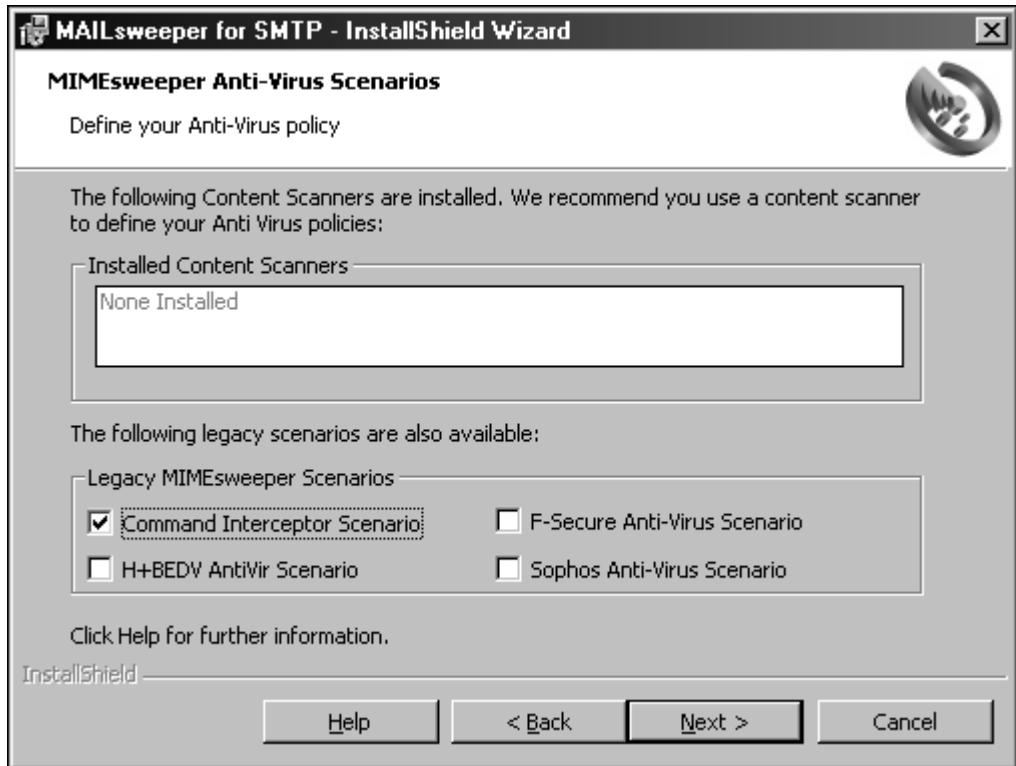
## INSTALLING THE COMMAND INTERCEPTOR SCENARIO

To install the Command Interceptor for MIMESweeper, you **must** first install the Command Interceptor Scenario. If you try to install the Command Interceptor before you install the scenario, the system displays an error message informing you that the Command Interceptor Scenario must be installed.

You can install the Command Interceptor Scenario during or after the installation of CS MAILsweeper 4.3 for SMTP.

### During the CS MAILsweeper Installation

To install the Command Interceptor Scenario during the installation of CS MAILsweeper 4.3 for SMTP, select the **Command Interceptor Scenario** check box under **Legacy MIMESweeper Scenarios** in the **MIMESweeper Anti-Virus Scenarios** dialog box:

**MIMesweeper Anti-Virus Scenarios Dialog Box**

## After the CS MAILsweeper Installation

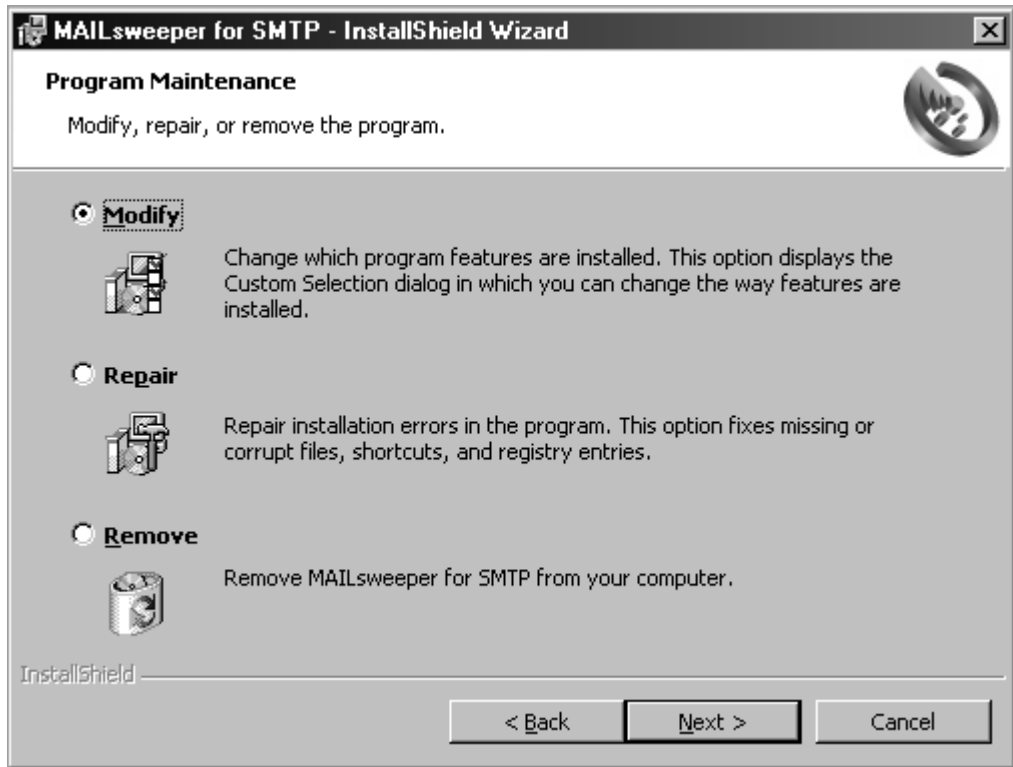
After you have installed CS MAILsweeper 4.3 for SMTP, you can install the Command Interceptor Scenario through the MAILsweeper installation program's **Program Maintenance** dialog box.



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

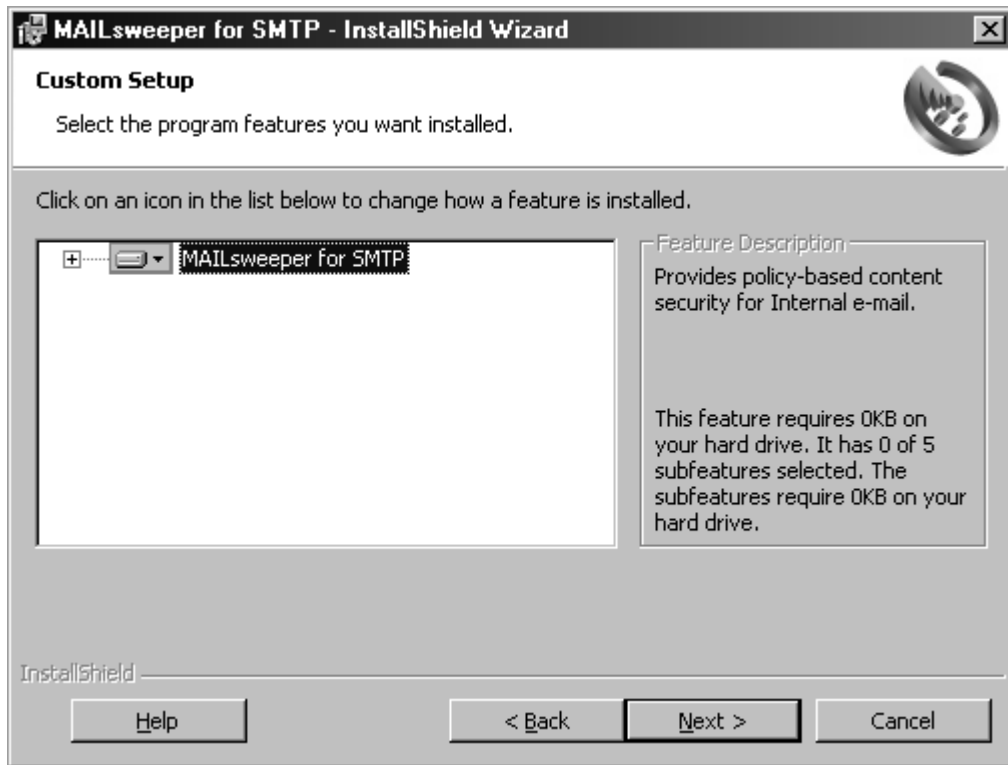
To install the Command Interceptor Scenario after the installation of CS MAILsweeper 4.3 for SMTP, follow these steps:

1. Click the **Start** button on the Windows taskbar.
2. Select **Settings**.
3. Click **Control Panel**.
4. Double-click **Add/Remove Programs**. The system displays the **Add/Remove Programs** dialog box.
5. Select **MAILsweeper for SMTP** from the list of currently installed programs, and click the **Change** button. The system displays the MAILsweeper for SMTP installation program's **Welcome** dialog box.
6. Click **Next**. The system displays the **Program Maintenance** dialog box:



**Program Maintenance Dialog Box**

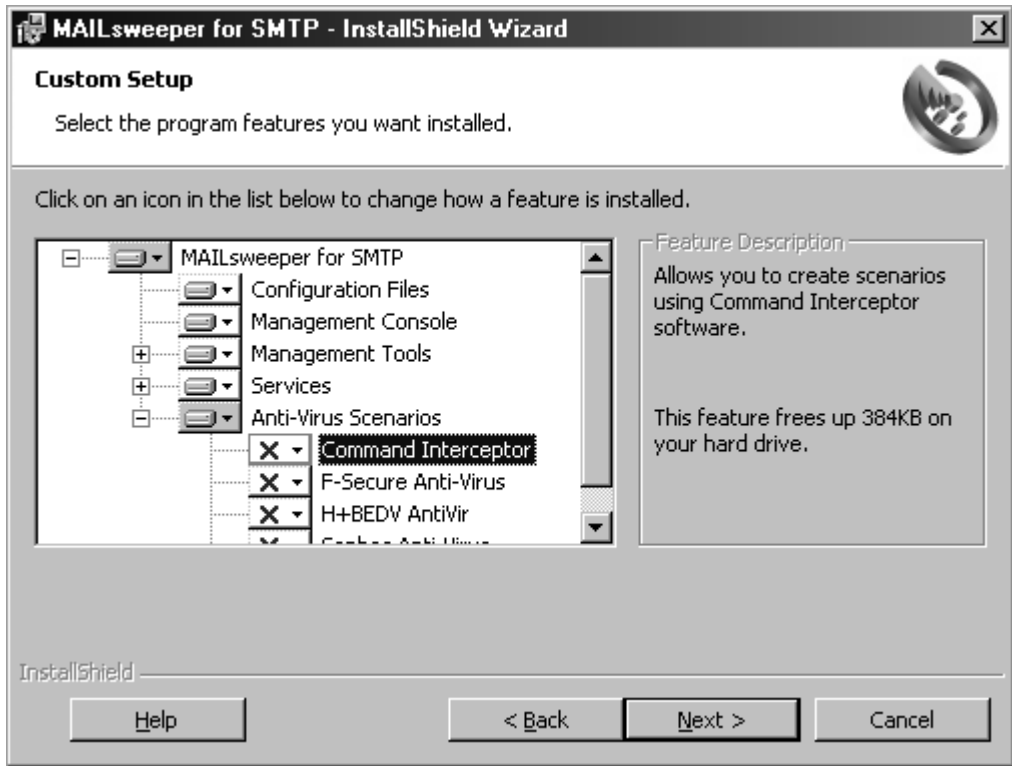
7. Select **Modify**, and click **Next**. The system displays the **Custom Setup** dialog box:




**Custom Setup Dialog Box**

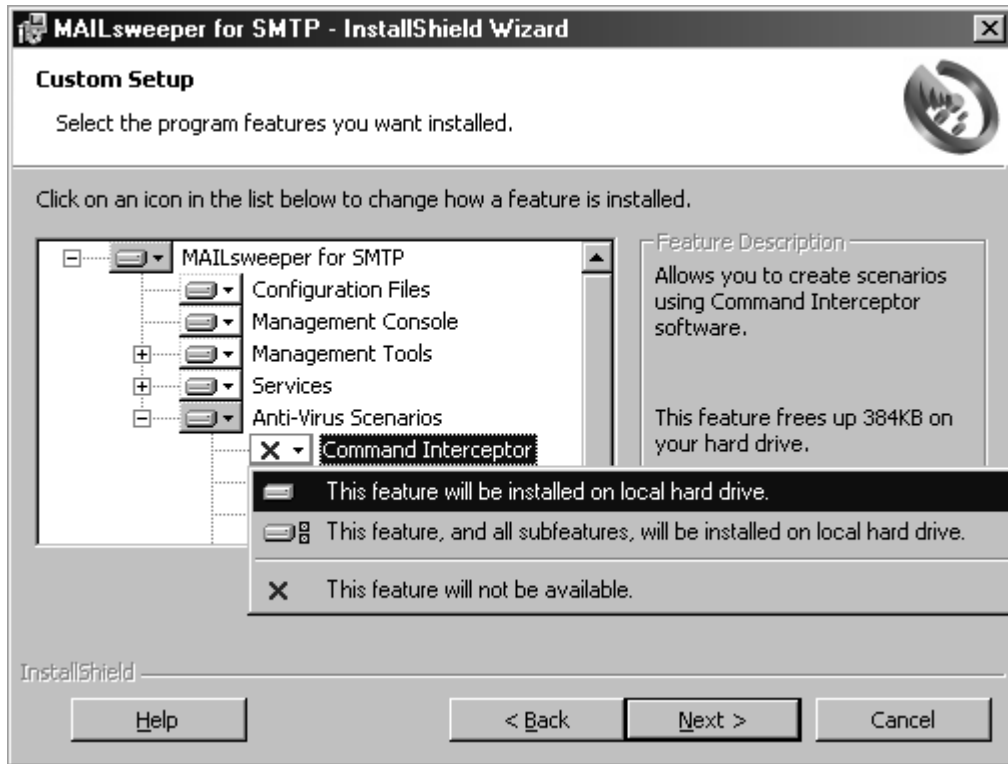
8. Click the plus sign (+) to the left of **MAILsweeper for SMTP** to expand it.
9. Click the plus sign (+) to the left of **Anti-Virus Scenarios** to display the scenarios:





Custom Setup Dialog Box – Anti-Virus Scenarios

10. Select **Command Interceptor**, and click the drop-down arrow  to the right of the icon. The system displays the installation state drop-down menu:



**Custom Setup Dialog Box – Installation State Drop-down Menu**

11. Select **This feature will be installed on local hard drive.**
12. Click **Next.** The system displays the **Ready to Modify the Program** dialog box.

13. Click **Install**. The system displays the **Installing MAILsweeper for SMTP** dialog box. Please wait while the program updates your system.



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

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

14. Click **Finish** to exit.

## INSTALLING COMMAND INTERCEPTOR

---

Adding the Command Interceptor to CS MAILsweeper 4.3 for SMTP is a four-step process.

1. Installing the Command Interceptor for MIMESweeper.
2. Creating a **Stripped** classification in MAILsweeper.



**NOTE:** Creating a **Stripped** classification in MAILsweeper allows you to create a Command Interceptor Scenario that deletes infected e-mail attachments that cannot be disinfected and then delivers the e-mail. For more information, refer to **Creating a Stripped Classification** located later in this chapter.

3. Creating and enabling the Command Interceptor Scenario.
4. Scheduling Command Interceptor virus definition file updates.

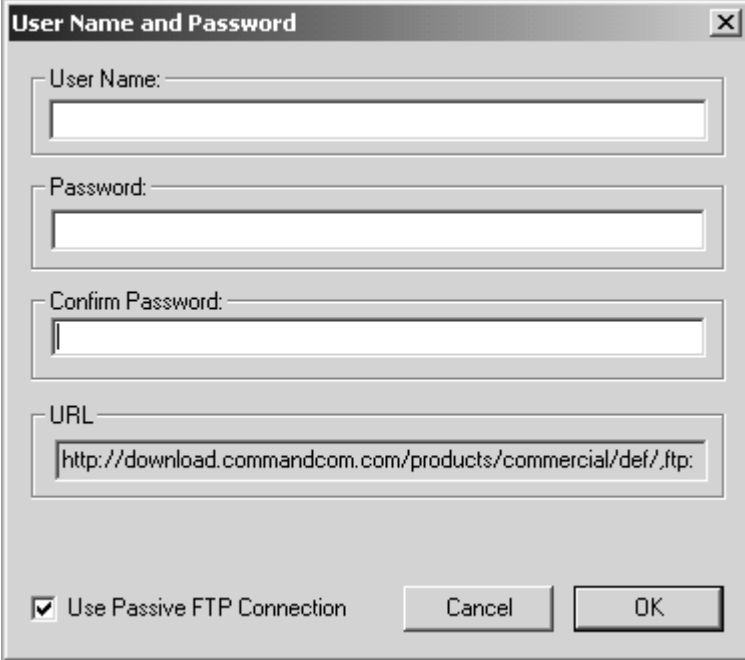
## INSTALLING COMMAND INTERCEPTOR FOR MIMESWEEPER

1. If you are installing the Command Interceptor for MIMESweeper from:
  - **the downloaded file** – on your system's hard drive, create a Command Interceptor installation folder. Move the downloaded file to this folder. Then, double-click the file. This extracts the Command Interceptor files. Go to **Step 2**.
  - **the CD** – place the CD into the CD-ROM drive, and change to that drive. Open the folder called **MSW4.3x**. Go to **Step 2**.
2. Open the **INTRCEPT** folder, and then double-click the file called **SETUP.EXE**. The system displays the **User Name and Password** dialog box.



**NOTE: Experienced Users Only** - You can also start the installation program by running the **msiexec** with the following parameters:

```
msiexec /i intrcept.msi REINSTALL=ALL REINSTALLMODE=vomus
```

A screenshot of a Windows-style dialog box titled "User Name and Password". The dialog box has a close button (X) in the top right corner. It contains four text input fields: "User Name:", "Password:", "Confirm Password:", and "URL:". The "URL:" field contains the text "http://download.commandcom.com/products/commercial/def/.ftp:". At the bottom left, there is a checked checkbox labeled "Use Passive FTP Connection". At the bottom right, there are two buttons: "Cancel" and "OK".

User Name and Password

User Name:

Password:

Confirm Password:

URL  
http://download.commandcom.com/products/commercial/def/.ftp:

Use Passive FTP Connection

Cancel OK

User Name and Password Dialog Box

3. In the **User Name** text box, type a **valid** Command Software Systems user name.
4. In the **Password** text box, type a **valid** Command Software Systems password.
5. In the **Confirm Password** text box, retype your password, and click **OK**. The system displays the **Updating System** dialog box.



**NOTE:** As some firewalls may have a problem with an active connection, the **Use Passive FTP Connection** check box is selected by default. If the URL specified in the **URL** text box is an FTP URL, the connection is made in passive mode. To use an active connection, clear the **Use Passive FTP Connection** check box.

When the installation is complete, the system displays a dialog box informing you that Command Interceptor for MIMESweeper has been successfully installed.

6. Click **Finish**.



**NOTE:** The following services will be started automatically:

- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security

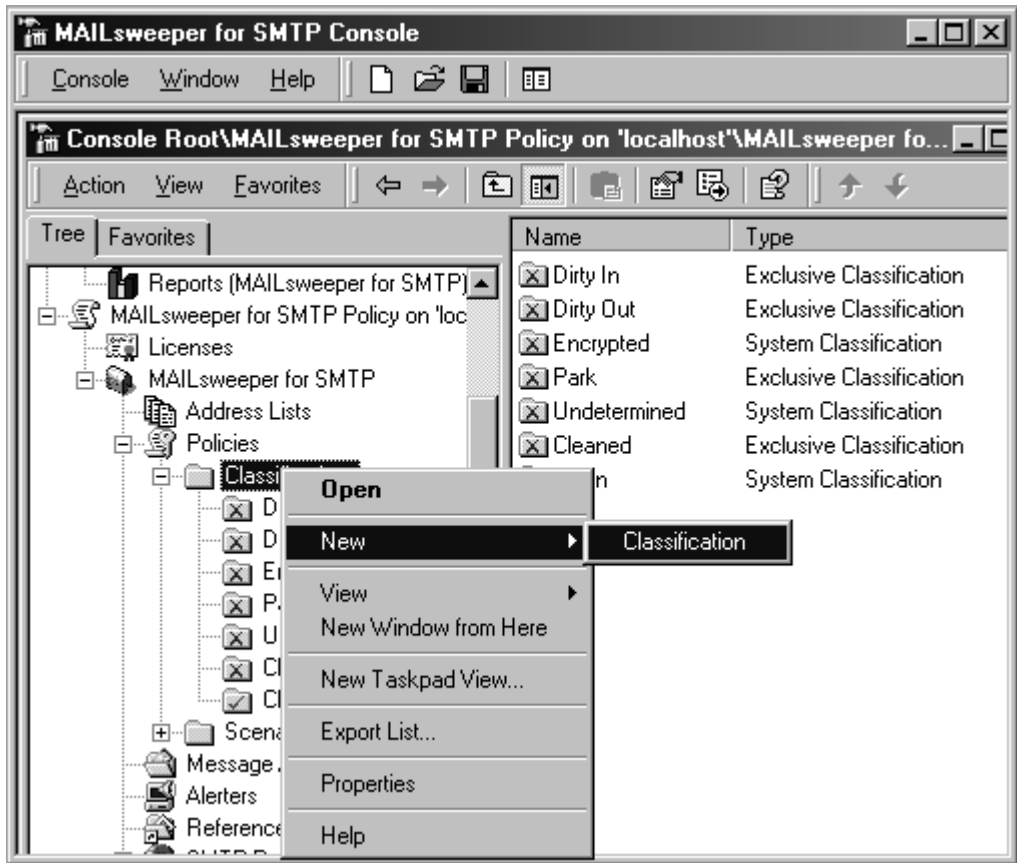
7. Go to **Creating a Stripped Classification**.

## CREATING A STRIPPED CLASSIFICATION

This section provides instructions on how to create a classification that deletes infected files that cannot be disinfected.

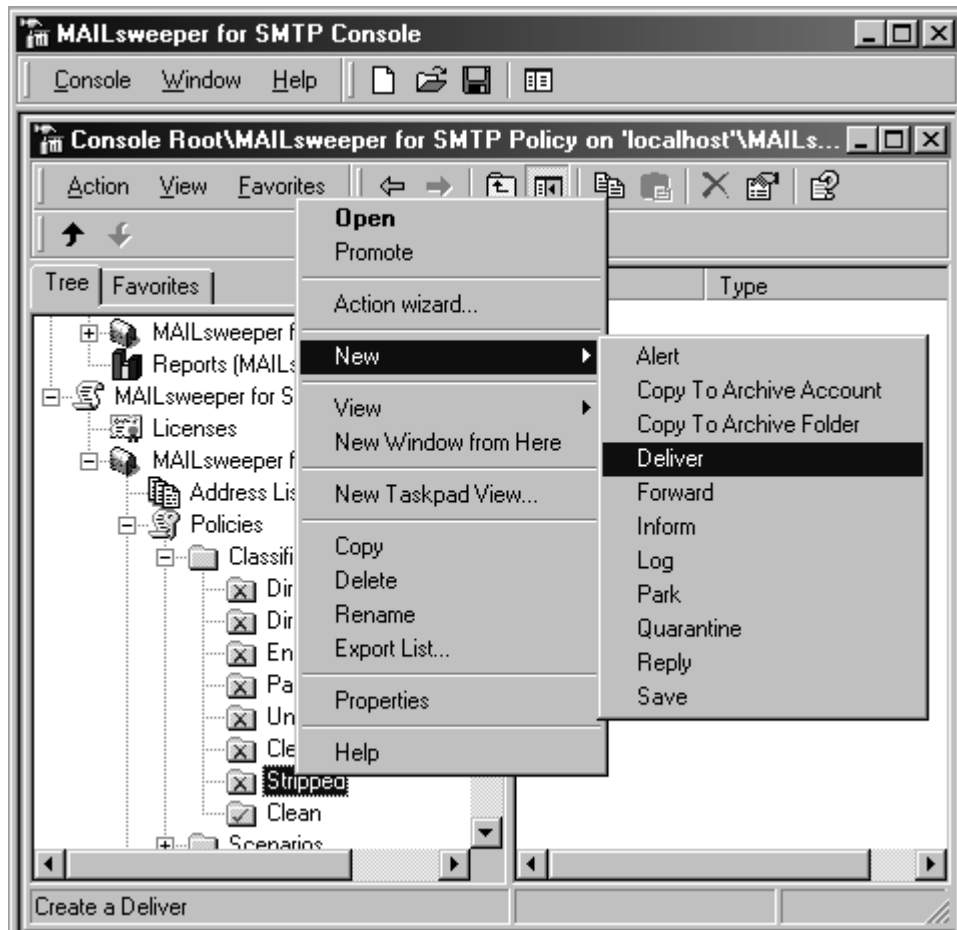
To create this classification follow these steps:

1. Open the **MAILsweeper for SMTP Console 4.3**.
2. In the **Tree** view, locate and select **Classifications**.
3. Click the plus sign (+) to the left of **Classifications** to expand it.
4. Using the right mouse button (right-click), click **Classifications**. The system displays a shortcut menu:



MAILsweeper for SMTP Console – Classifications Shortcut Menu

5. Select **New**, and click **Classification**. In the **Tree**, the system creates a new classification called **Classification** with a text box around the name.
6. Type **Stripped**, and press **Enter**.  
Now you need to create a **Deliver** action for the **Stripped** classification so that messages are placed in the delivery queue for delivery to the recipients.
7. Right-click the **Stripped** classification. The system displays a shortcut menu:



**Stripped Classification Shortcut Menu – Deliver Action**

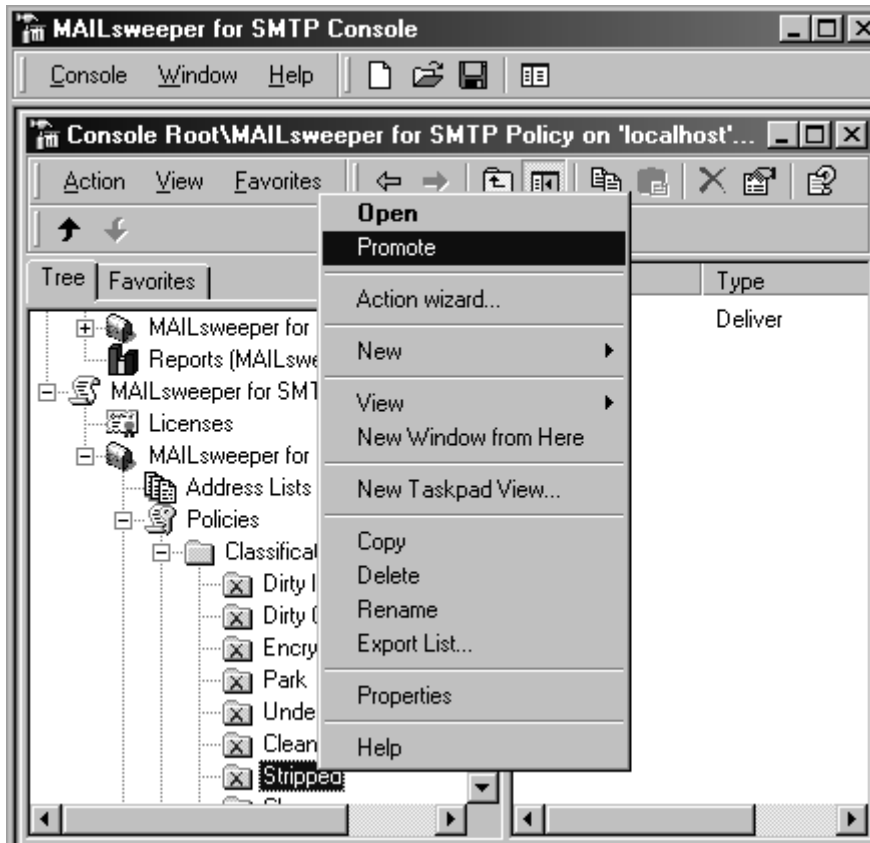


8. Select **New**, and click **Deliver**. The system displays the **Deliver Wizard Welcome** dialog box.

Follow the wizard's on-screen instructions. When the system displays the **Action Name** dialog box, accept **Deliver** as the name for this new action. When the wizard is complete, the systems adds the **Deliver** action to the right pane.

As classifications are applied in hierarchical order, you now need to promote or demote the **Stripped** classification in the **Classifications** branch so that it is located just beneath the **Cleaned** classification.

9. Right-click the **Stripped** classification. The system displays a short-cut menu:



**Stripped Classification Shortcut Menu – Promote**

10. Click **Promote**. This moves the **Stripped** classification above the immediately preceding classification.



**NOTE:** If the **Stripped** classification is above the **Cleaned** classification, click **Demote** to move the **Stripped** classification beneath the classification that immediately follows.

11. Repeat Steps **9** and **10** until the **Stripped** classification is located just beneath the **Cleaned** classification.



**NOTE:** The **Stripped** classification customizations do **not** apply until you stop and then start the following services:

- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security

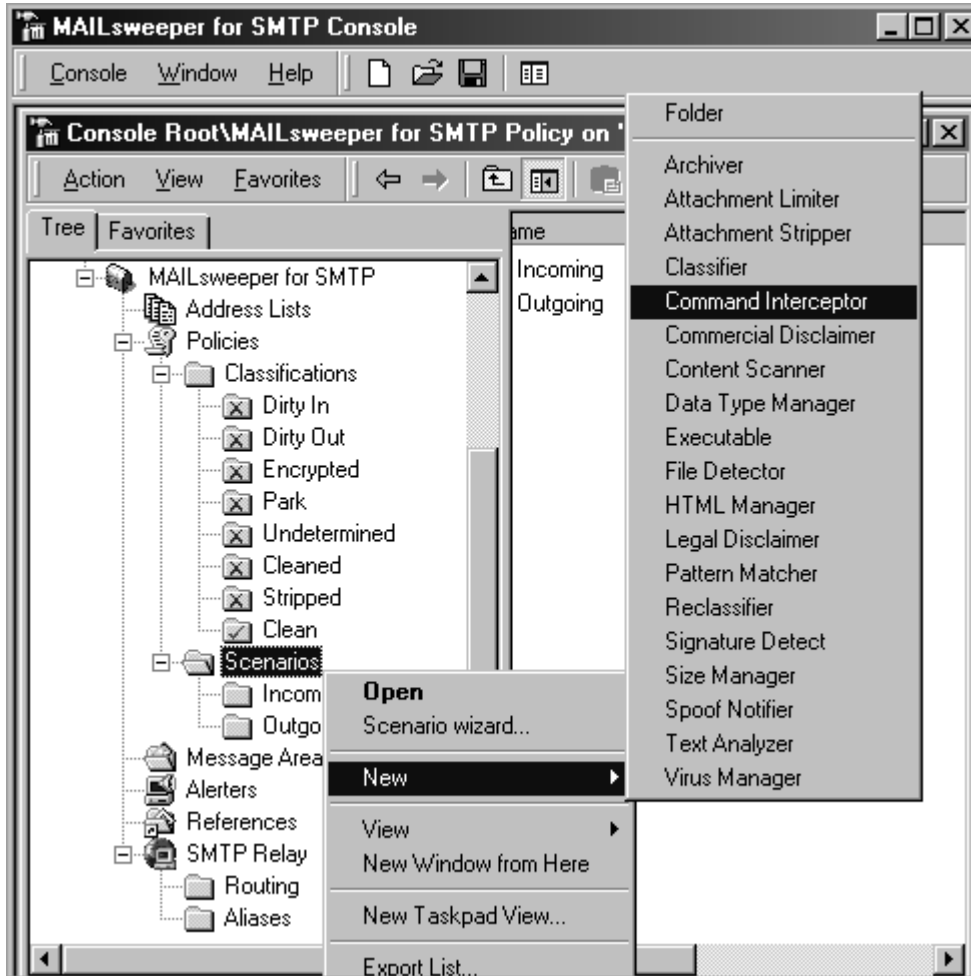
As the customizations to the Command Interceptor Scenario also require that you stop and start these services, we recommend that you do so after you create and enable the scenario.

12. Go to **Creating And Enabling The Command Interceptor Scenario**.

## CREATING AND ENABLING THE COMMAND INTERCEPTOR SCENARIO

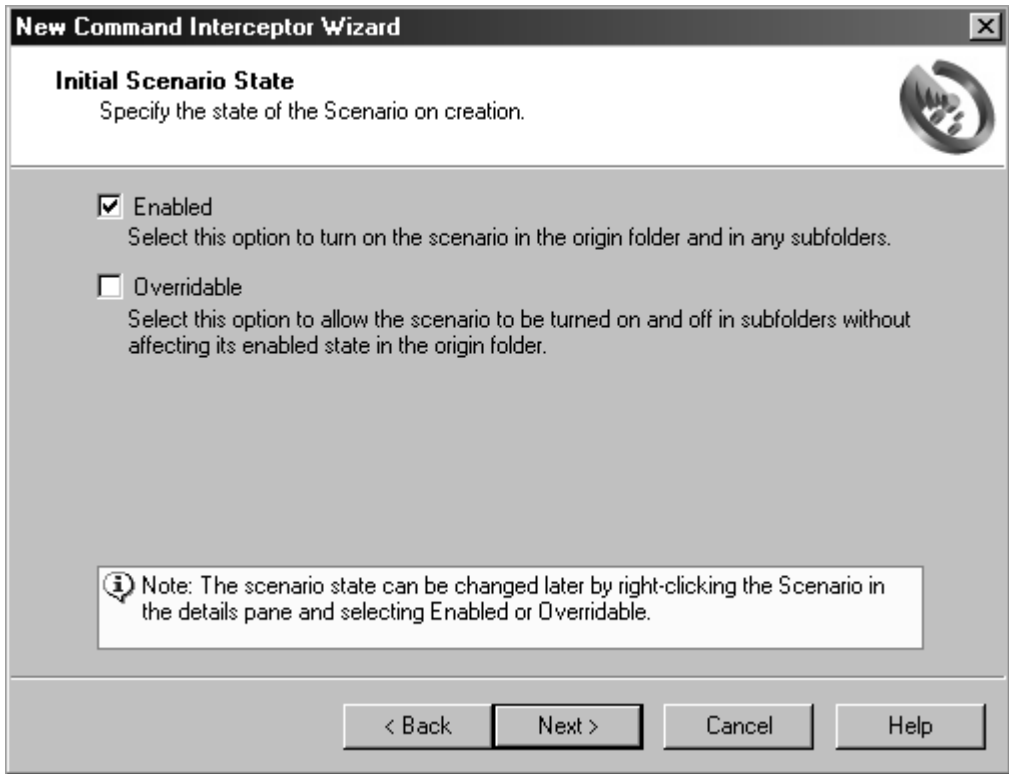
To create and enable the Command Interceptor Scenario, follow these steps:

1. Open the **MAILsweeper for SMTP Console 4.3**.
2. In the **Tree** view, locate and select **Scenarios**.
3. Click the plus sign (+) to the left of **Scenarios** to expand it.
4. Right-click **Scenarios**. The system displays a shortcut menu:



**Scenario Shortcut Menu**

5. Select **New**, and then click **Command Interceptor**. The system displays the **Command Interceptor Wizard Welcome** dialog box.
6. Click **Next**. The system displays the **Initial Scenario State** dialog box:



Initial Scenario State Dialog Box

7. Select the **Enabled** check box to turn on the scenario.



**NOTE:** You can change the state of the scenario at a later time by right-clicking the Command Interceptor Scenario in the right pane of the **MAILsweeper for SMTP Console**. Just select or clear the **Enabled** shortcut menu item.

8. Clear the **Overridable** check box.
9. Click **Next**. The system displays **Location** dialog box:



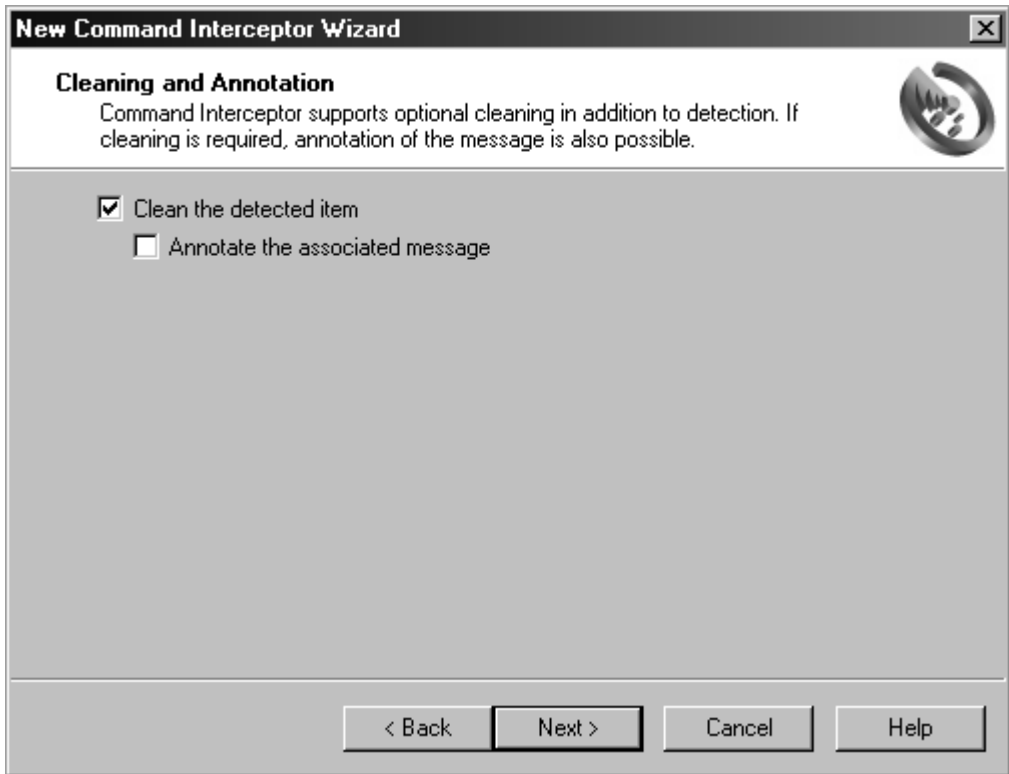
Location Dialog Box

10. In the **Enter the location of Command Interceptor** text box, type where you want to install the Command Interceptor files.



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

11. Click **Next**. The system displays the **Cleaning and Annotation** dialog box:



**Cleaning and Annotation Dialog Box**

12. Select the **Clean the detected item** check box. This option automatically attempts to disinfect a virus when it is found.



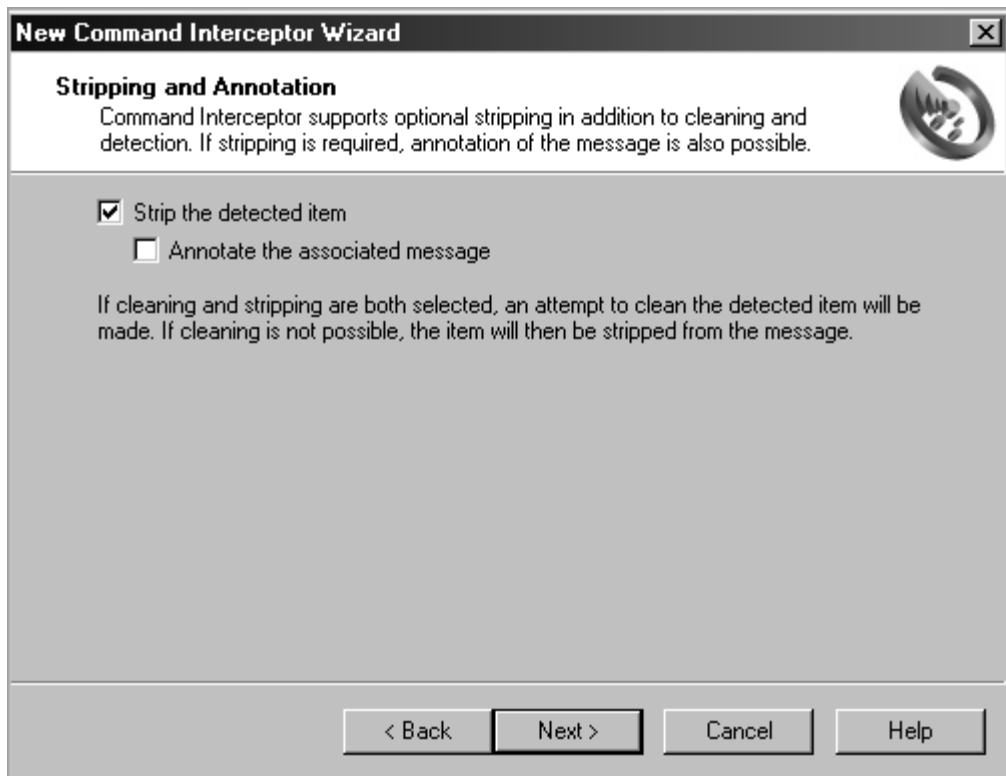
**NOTE:** You can also add text to the original message when the virus is disinfecting by selecting the **Annotate the associated message** check box. For example, you may want to indicate that has virus has been disinfecting.

13. Click **Next**. The system displays the **Stripping and Annotation** dialog box:



**NOTE:** If you selected the **Annotate the associated message** check box, the system first displays the **Annotate Text** dialog box.

In the **Annotation** text box, type the message that you want to add, for example, *A virus has been cleaned*, and click **Next**. The system displays the **Annotation Position** dialog box. Select where you want to insert the text, for example at the beginning or at the end of the message, and click **Next**.



**Stripping and Annotation Dialog Box**



14. Select the **Strip the detected item** check box. If it is not possible to disinfect the infected attachment, this option removes the infected attachment from the message.



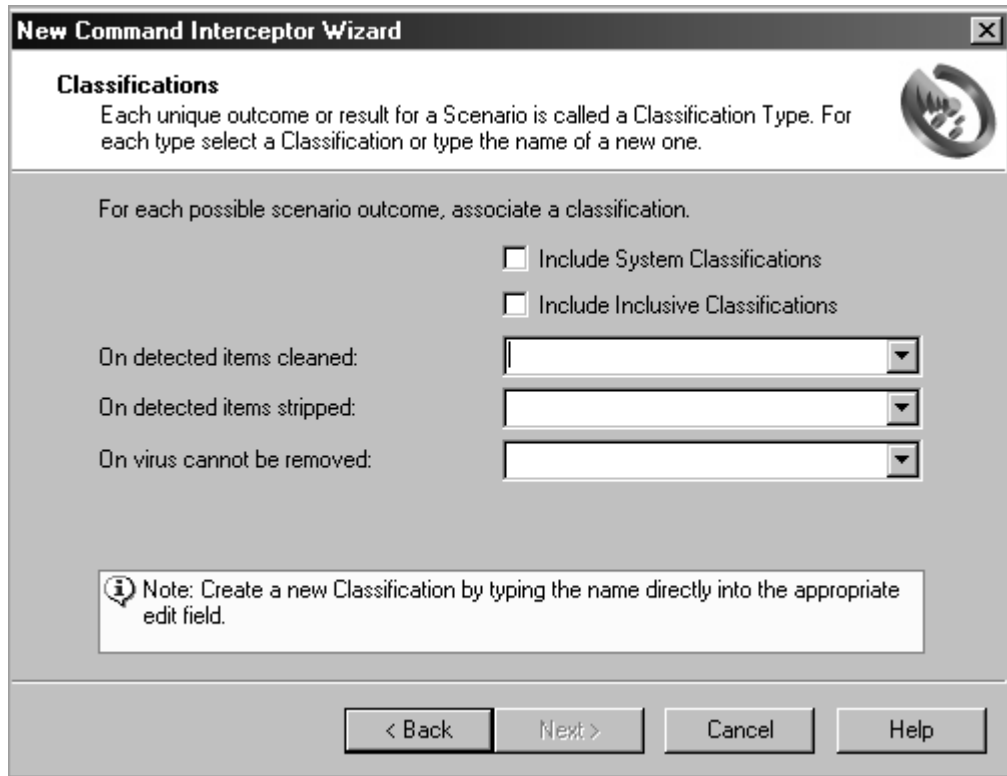
**NOTE:** You can also add text to the original message when the virus is removed by selecting the **Annotate the associated message** check box. For example, you may want to indicate that an infected attachment has been removed.

15. Click **Next**. The system displays the **Classifications** dialog box:



**NOTE:** If you selected the **Annotate the associated message** check box, the system first displays the **Annotate Text** dialog box.

In the **Annotation** text box, type the message that you want to add, for example, *A potentially dangerous attachment has been stripped*, and click **Next**. The system displays the **Annotation Position** dialog box. Select where you want to insert the text, for example at the beginning or at the end of the message, and click **Next**.



**New Command Interceptor Wizard**

### Classifications

Each unique outcome or result for a Scenario is called a Classification Type. For each type select a Classification or type the name of a new one.

For each possible scenario outcome, associate a classification.


Include System Classifications

Include Inclusive Classifications

On detected items cleaned:

On detected items stripped:

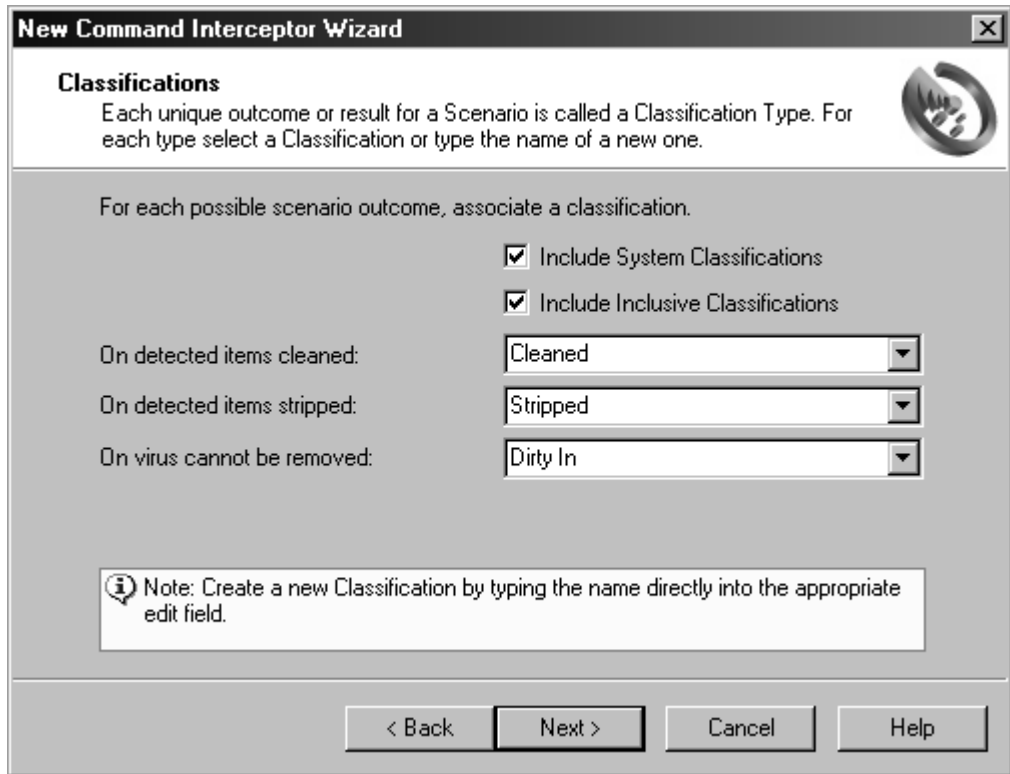
On virus cannot be removed:

 Note: Create a new Classification by typing the name directly into the appropriate edit field.

< Back   Next >   Cancel   Help

**Classifications Dialog Box**

16. Select the **Include System Classifications** check box.
17. Select the **Include Inclusive Classifications** check box.
18. From the **On detected items cleaned** list, select **Cleaned**.
19. From the **On detected items stripped** list, select **Stripped**.
20. From the **On virus cannot be removed** list, select **Dirty In**.



**Classifications Dialog Box – Classifications Selected**

21. Click **Next**. The system displays the **Scenario Name** dialog box:



**New Command Interceptor Wizard**

**Scenario Name**  
Enter a name for the new item with a comment if required.

Name:  
Command Interceptor

Notes:

< Back   Next >   Cancel   Help

Scenario Name Dialog Box



**NOTE:** If you want to change the default name of the scenario, **Command Interceptor**, in the **Name** text box, type a new name.

22. Click **Next**. The system displays the **Completing the Command Interceptor Wizard** dialog box.
23. Click **Finish**.

You can now configure the alerting mechanisms for the classifications listed in the **Classifications** branch.

To configure these mechanisms, follow these steps:

1. Right-click a classification.
2. Select **New** from the shortcut menu.
3. Select **Notification**. The system displays a shortcut menu with the **Alert**, **Inform**, **Log**, and **Reply** options.
4. For details on how to configure these options, see the product's online help or refer to the *MAILsweeper for SMTP Version 4.0 Getting Started Guide*.



For the **Stripped** classification and the Command Interceptor Scenario customizations to apply, you **must** stop and then start the following services:

- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security



To keep your virus protection up-to-date, we highly recommend that you update your Command Interceptor virus definition files (deffiles).

You can schedule updates to occur automatically, or you can manually update these files. To schedule updates, refer to **Scheduling Command Interceptor Definition File Updates**. To update manually, refer to **Updating the Command Interceptor Definition Files Manually**.

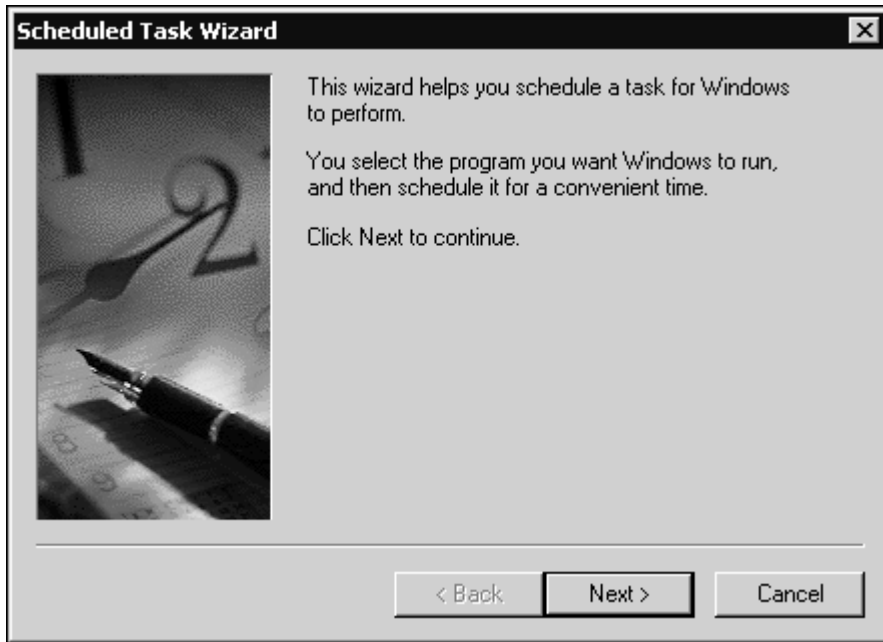
## SCHEDULING COMMAND INTERCEPTOR DEFINITION FILE UPDATES



**NOTE:** You can also update the Command Interceptor definition files manually. For more information, refer to **Updating the Command Interceptor Definition Files Manually**.

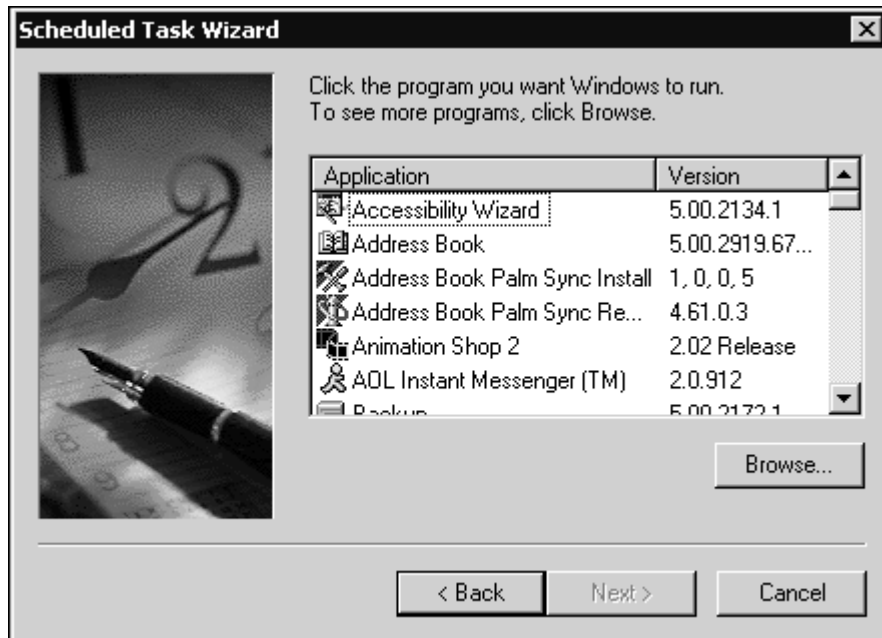
To schedule updates of the Command Interceptor definition files, follow these steps:

1. Click the **Start** button on the Windows taskbar.
2. Select **Settings**.
3. Click **Control Panel**.
4. Double-click **Scheduled Tasks**. The system displays the **Scheduled Tasks** folder.
5. Double-click **Add Scheduled Tasks**. The system displays the Windows **Scheduled Task Wizard Main** dialog box:



Scheduled Task Wizard Main Dialog Box

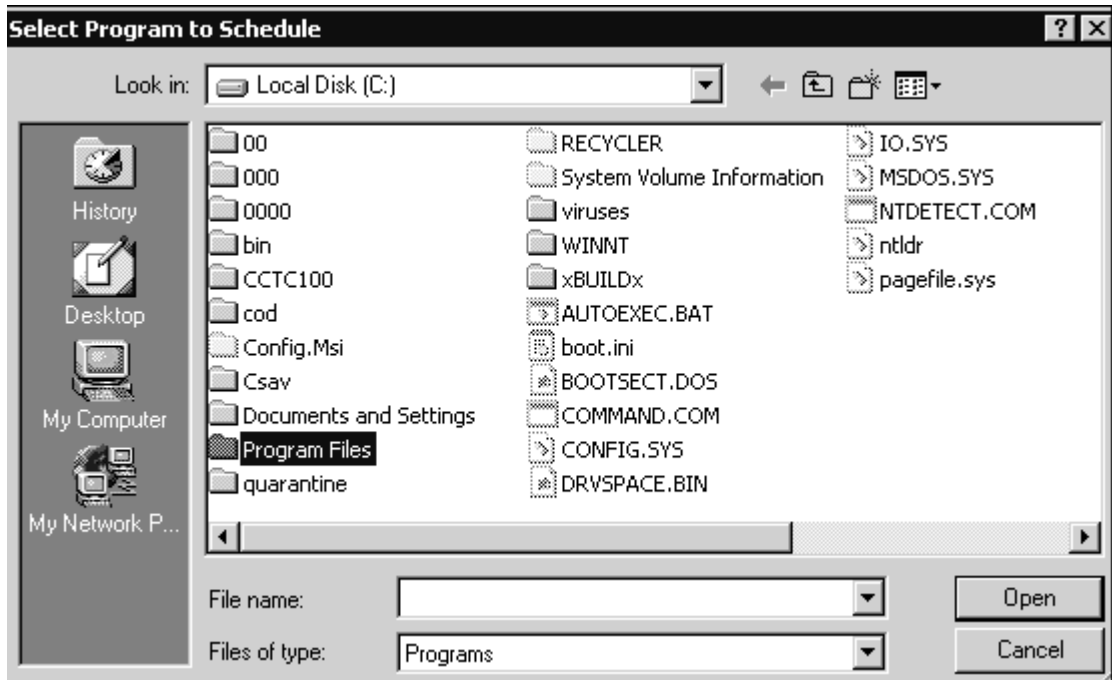
6. Click **Next** to continue. The system displays a **Program Selection** dialog box:



Program Selection Dialog Box

7. Click **Browse**. The system displays the **Select Program to Schedule** dialog box:





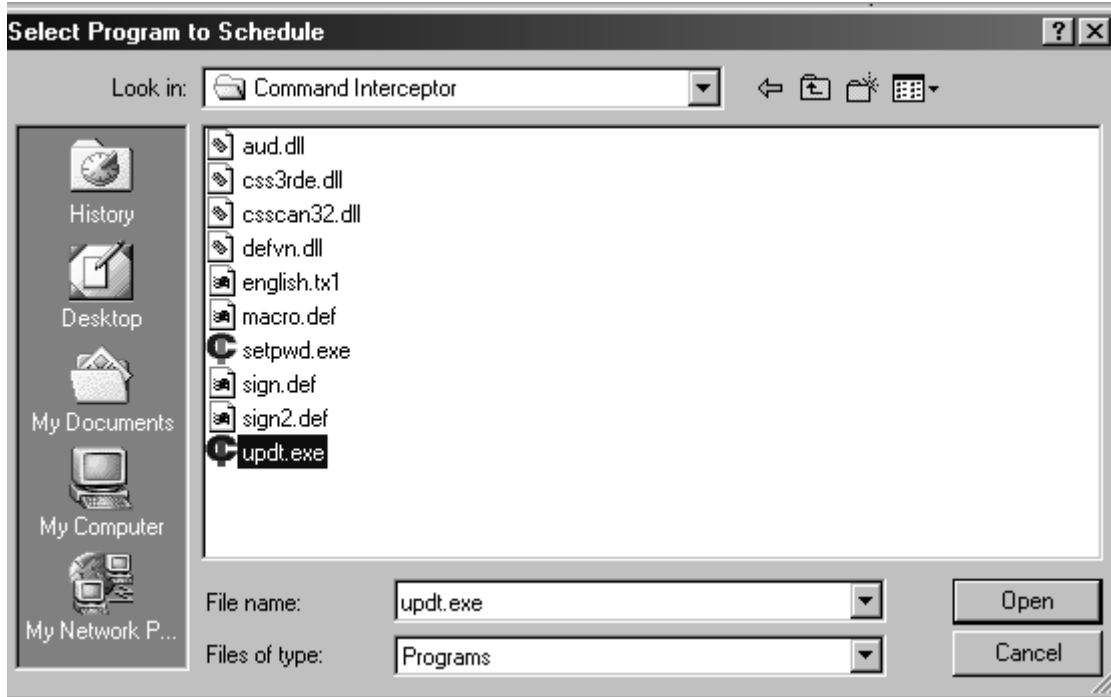
Select Program to Schedule Dialog Box

8. Double-click **Program Files**. The system displays the **Program Files** folder.



**NOTE:** If you have upgraded from MAILsweeper for SMTP 4.2, double-click **Common Files**, and then **Content Technologies**. The system displays the **Content Technologies** folder. Go to **Step 12**.

9. Double-click **Command Software**. The system displays the **Command Software** folder.
10. Double-click **MIMESweeper**. The system displays the **MIMESweeper** folder.
11. Double-click **Command Interceptor**. The system displays the Command Interceptor folder:



**Select Program to Schedule Dialog Box – Command Interceptor Folder**

12. Select **updt.exe**, and click **Open**. The system displays a **Task Name and Frequency** dialog box:



**Task Name and Frequency Dialog Box**

13. Select how often you want to perform this task, for example, **Daily**, **Weekly**, **Monthly**, and click **Next**. The system displays a **Time and Day** dialog box:



**Time and Day Dialog Box**

14. In the **Start time** box, select the time of day that you want the update to take place, for example, 1:43 AM.
15. Under **Perform this task**, select the days that you want the update to take place, for example, **Every Day**, **Weekdays**, **Every 5 days**.
16. In the **Start date** box, select the date that you want the updates to start, and click **Next**. The system displays a **User Name and Password** dialog box:



**Scheduled Task Wizard**

Enter the name and password of a user. The task will run as if it were started by that user.

Enter the user name:

Enter the password:

Confirm password:

< Back    Next >    Cancel

**User Name and Password Dialog Box**

17. In the **Enter the user name** text box, type a local user name that has Administrative rights.
  18. In the **Enter the password** text box, type the password of the local user name.
  19. In the **Confirm password** text box, retype the password, and click **Next**. The system displays a **Scheduled Task Complete** dialog box:
-



**Scheduled Task Complete Dialog Box**

20. Click **Finish**.

## UPDATING THE COMMAND INTERCEPTOR DEFINITION FILES MANUALLY

To keep your product's anti-virus abilities up-to-date, please check Command Software System's web site at <http://www.commandsoftware.com/html/defupdate.html>. There, you can download the latest Command Interceptor definition files.

To update the files, follow these steps:



**NOTE:** The following services will be stopped and restarted automatically:

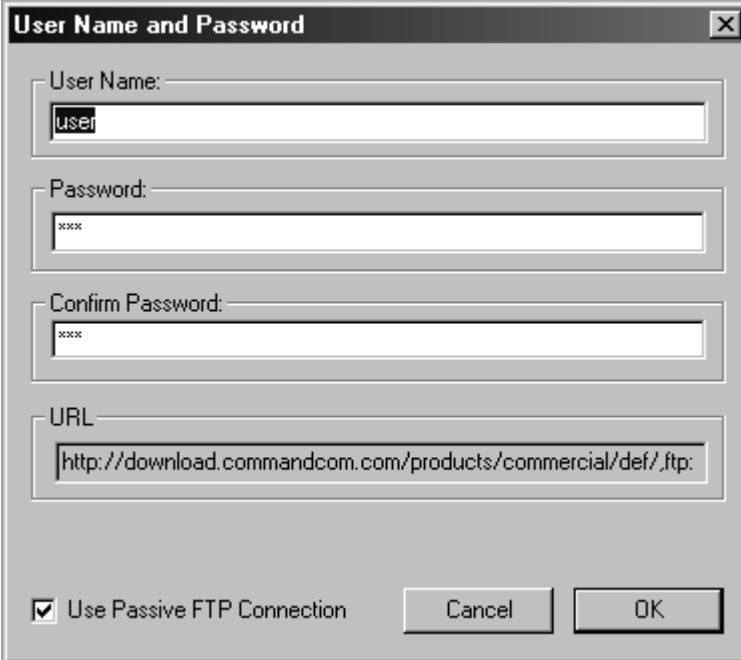
- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security

1. On your system's hard drive, create a temporary folder.
2. Download the file called **DEFINT.MSP** from the Command Software System's web site to the temporary folder that you created in **Step 1**.
3. Double-click the file. This updates the Command Interceptor definition files.
4. Delete the file called **DEFINT.MSP**.

## CHANGING YOUR COMMAND INTERCEPTOR FOR MIMESWEEPER PASSWORD

---

1. Go to the Command Interceptor installation folder.
2. Open the **INTRCEPT** folder, and then double-click the file called **SETUP.EXE**. The system displays the **User Name and Password** dialog box:



The dialog box titled "User Name and Password" contains the following fields and controls:

- User Name:** A text box containing the text "User".
- Password:** A text box containing three asterisks "xxx".
- Confirm Password:** A text box containing three asterisks "xxx".
- URL:** A text box containing the text "http://download.commandcom.com/products/commercial/def/,ftp:". Below this field is a small, faint URL "http://download.commandcom.com/products/commercial/def/,ftp:".
- Use Passive FTP Connection:** A checkbox that is checked.
- Buttons:** "Cancel" and "OK" buttons.

**User Name and Password Dialog Box**

3. In the **User Name** text box, type a **valid** Command Software Systems user name.
4. In the **Password** text box, type a **valid** Command Software Systems password.



5. In the **Confirm Password** text box, retype your password, and click **OK**. The system displays the **Updating System** dialog box.



**NOTE:** As some firewalls may have a problem with an active connection, the **Use Passive FTP Connection** check box is selected by default. If the URL specified in the **URL** text box is an FTP URL, the connection is made in passive mode. To use an active connection, clear the **Use Passive FTP Connection** check box.

When the installation is complete, the system displays a dialog box informing you that Command Interceptor for MIMESweeper has been successfully installed.

6. Click **Finish**.

## REMOVING COMMAND INTERCEPTOR FOR MIMESWEEPER

---

To remove the Command Interceptor for MIMESweeper, follow these steps:

1. Open the **MAILsweeper for SMTP Console**.
2. In the **Tree** view, locate and select **Scenarios**.
3. Delete any Command Interceptor scenarios.
4. Close the **Console**.
5. Using the **Add/Remove Programs** feature in the Windows Control Panel, first remove **Command Interceptor for MIMESweeper**.
6. Then, using the MAILsweeper for SMTP installation's **Program Maintenance** dialog box, remove the **Command Interceptor Scenario**. For more information, refer to **Removing An Anti-virus Scenario** located later in this chapter.

7. Restart the following services:

- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security



**NOTE:** If you have scheduled updates of the Command Interceptor definition files through the Windows® Scheduled Task Wizard, you also need to delete the scheduled task.

To delete the scheduled task, follow these steps:

1. Click the **Start** button on the Windows taskbar.
2. Select **Settings**.
3. Click **Control Panel**.
4. Double-click **Scheduled Tasks**.
5. Right-click the **UPDT** task. The system displays a drop-down menu.
6. Click **Delete**. The system displays the **Confirm File Delete** dialog box.
7. Click **Yes**.

## REMOVING AN ANTI-VIRUS SCENARIO

---

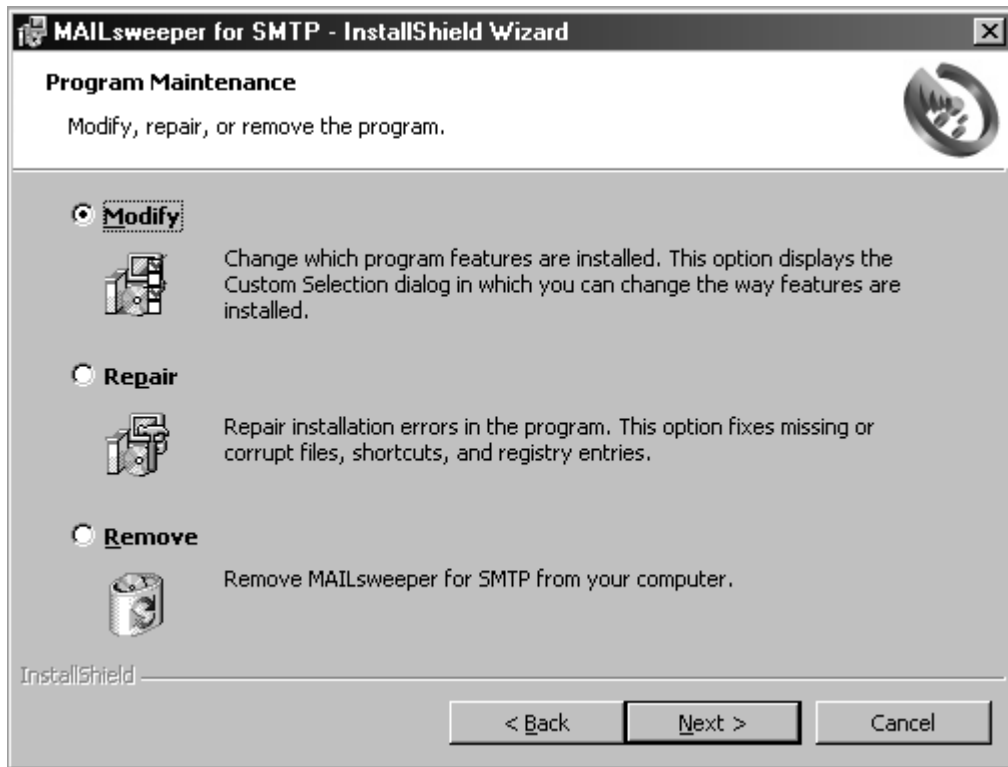
After you have installed CS MAILsweeper 4.3 for SMTP, you can remove an anti-virus scenario through the MAILsweeper installation program's **Program Maintenance** dialog box.



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

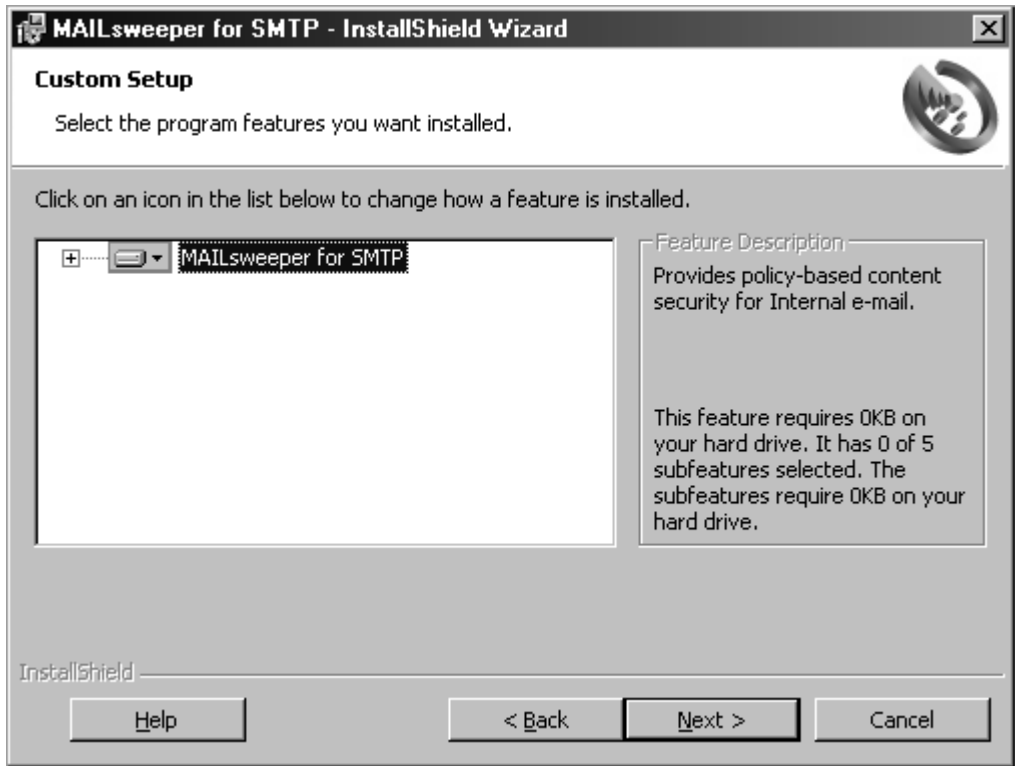
To remove an anti-virus scenario after the installation of CS MAILsweeper 4.3 for SMTP, follow these steps:

1. Click the **Start** button on the Windows taskbar.
2. Select **Settings**.
3. Click **Control Panel**.
4. Double-click **Add/Remove Programs**. The system displays the **Add/Remove Programs** dialog box.
5. Select **MAILsweeper for SMTP** from the list of currently installed programs, and click the **Change** button. The system displays the installation program's **Welcome** dialog box.
6. Click **Next**. The system displays the **Program Maintenance** dialog box:



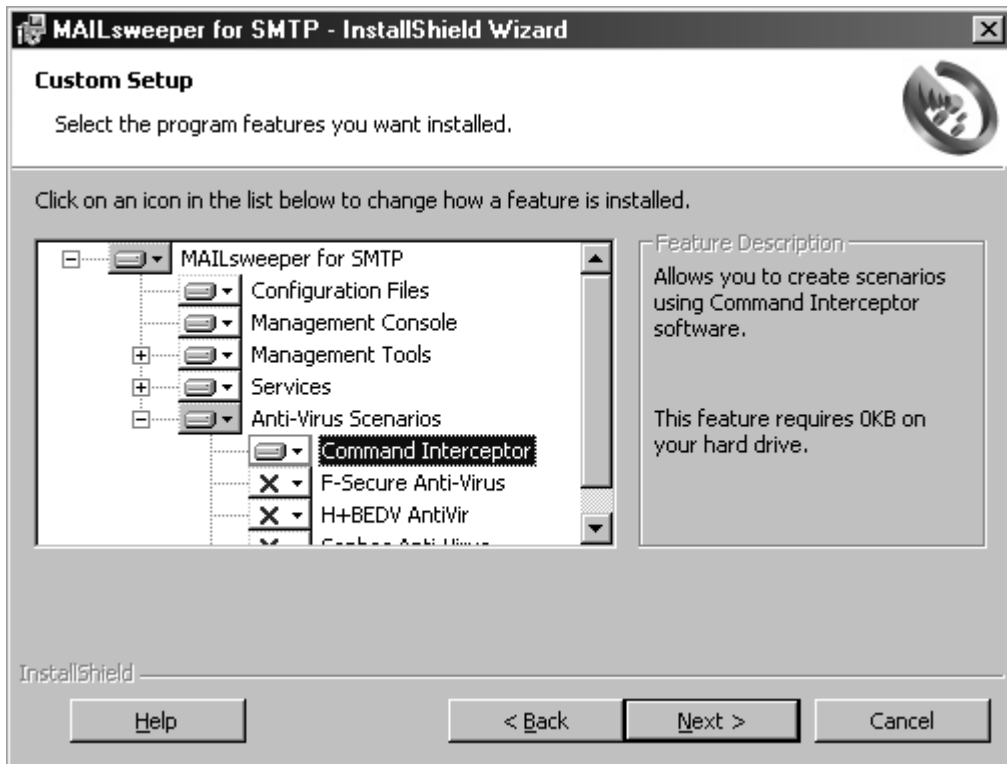
**Program Maintenance Dialog Box**

7. Select **Modify**, and click **Next**. The system displays the **Custom Setup** dialog box:




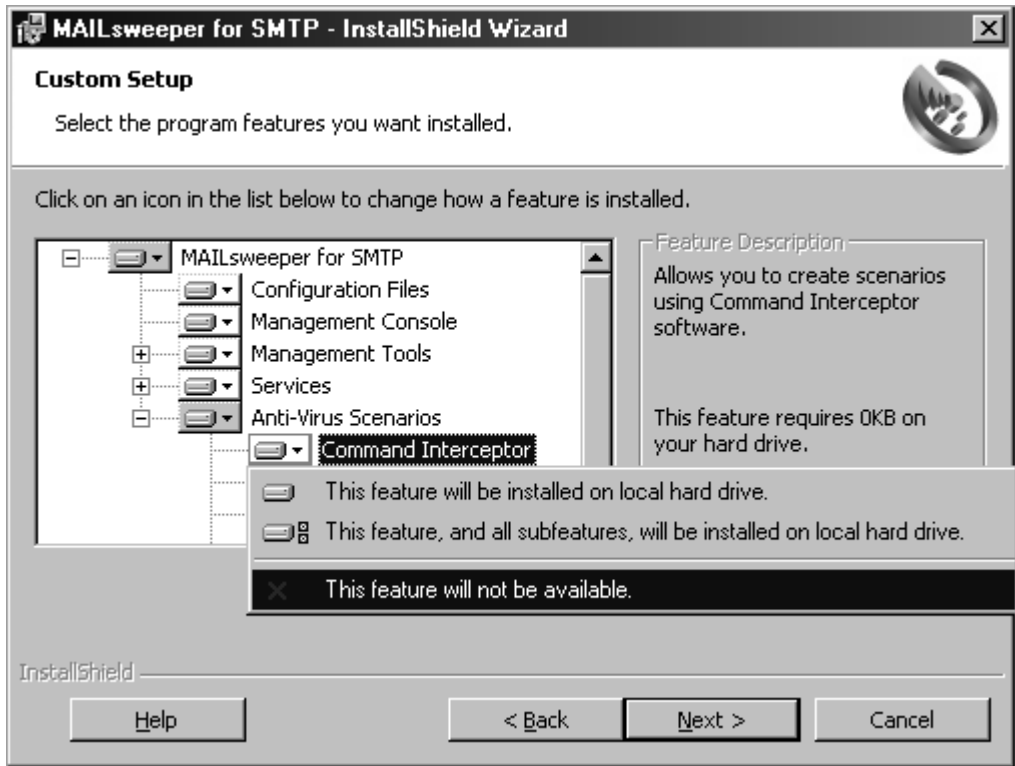
Custom Setup Dialog Box

8. Click the plus sign (+) to the left of **MAILsweeper for SMTP** to expand it.
9. Click the plus sign (+) to the left of **Anti-Virus Scenarios** to display the scenarios.



**Custom Setup Dialog Box – Anti-Virus Scenarios**

10. Select the anti-virus scenario that you want to remove, and click the drop-down arrow  to the right of the icon. The system displays the installation state drop-down menu:



Installation State Drop-down Menu

11. Select **This feature will not be available**.
12. Click **Next**. The system displays the **Ready to Modify the Program** dialog box.
13. Click **Install**. The system displays the **Installing MAILsweeper for SMTP** dialog box. Please wait while the program updates your system.



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

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

14. Click **Finish** to exit.



# MAILSWEEPER 4.2 FOR SMTP



To enable Command Interceptor protection, you must install the Command AntiVirus Scenario for MAILsweeper™ and the Command Interceptor™ for MIMESweeper™. The instructions in this chapter can be used to install them from the downloaded file or from the CD.

## PRE-INSTALLATION REQUIREMENTS

---

Before installing the Command Interceptor for MIMESweeper, your system must:

- Have MAILsweeper 4.2 For SMTP installed on an NTFS-formatted partition
- Not have any e-mail anti-virus program installed



**NOTE:** To remove a previously installed e-mail anti-virus program, use the **Add/Remove Programs** feature in the Windows NT® Control Panel.

If your system does not meet the above-mentioned requirements, Command Interceptor may not function correctly.

---

## INSTALLING

---

Adding Command Interceptor to MAILsweeper is a four-step process.

1. Installing the Command AntiVirus Scenario.
2. Installing the Command Interceptor for MIMESweeper.
3. Scheduling Command Interceptor Definition File Updates.
4. Enabling the Command AntiVirus Scenario.



**NOTE:** You can also create a Delete classification in MAILsweeper to delete infected files that cannot be disinfected. For more information, refer to **Creating a Delete Classification** located later in this chapter.

## INSTALLING THE COMMAND ANTIVIRUS SCENARIO

To install the Command AntiVirus Scenario, follow these steps:

1. Open the **MAILsweeper for SMTP Console**.
2. In the **Tree** view, locate and click **Services**.
3. In the left pane, select the following services:
  - MAILsweeper for SMTP Delivery
  - MAILsweeper for SMTP Receiver
  - MAILsweeper for SMTP Security
4. Using the right mouse button (right-click), click the selected service(s), and on the drop-down menu, click **Stop**.

5. If you are installing the Command AntiVirus Scenario from:
  - **the downloaded file** – On your system's hard drive, create a Command Interceptor installation folder. Move the downloaded file to this folder. Then, double-click the file. This extracts the Command Interceptor files. Go to **Step 6**.
  - **the CD** – Place the CD into the CD-ROM drive and change to that drive. Open the folder called **MSW4.2x**. Go to **Step 6**.
6. Open the **MAILSCEN** folder, and then double-click the file called **SETUP.EXE**. The system displays a **Welcome** screen.
7. Click **Next** to continue. Follow the instructions in the dialog boxes.
8. When the installation is complete, go to **Installing Command Interceptor for MIMESweeper**.

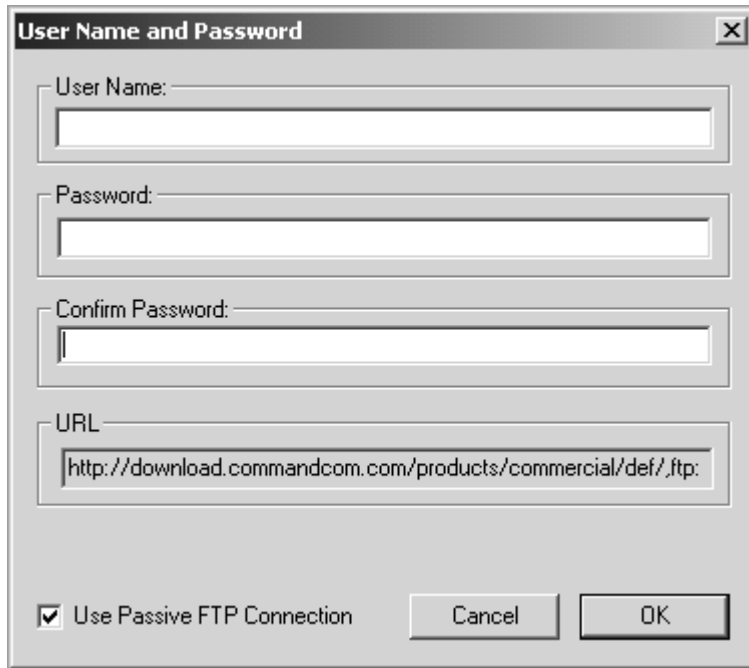
## INSTALLING COMMAND INTERCEPTOR FOR MIMESWEEPER

1. If you are installing the Command Interceptor for MIMESweeper from:
  - **the downloaded file** – go to the Command Interceptor installation folder that you created in **Step 5 of Installing the Command AntiVirus Scenario**, and open that folder. Then go to **Step 2**.
  - **the CD** – place the CD into the CD-ROM drive and change to that drive. Open the folder called **MSW4.2x**. Go to **Step 2**.
2. Open the **INTRCEPT** folder, and then double-click the file called **SETUP.EXE**. The system displays the **User Name and Password** dialog box.



**NOTE: Experienced Users Only** - You can also start the installation program by running the **msiexec** with the following parameters:

```
msiexec /i intrcept.msi REINSTALL=ALL REINSTALLMODE=vomus
```



The image shows a dialog box titled "User Name and Password" with a close button (X) in the top right corner. It contains four text input fields: "User Name:", "Password:", "Confirm Password:", and "URL:". The "URL:" field contains the text "http://download.commandcom.com/products/commercial/def/.ftp:". At the bottom left, there is a checked checkbox labeled "Use Passive FTP Connection". At the bottom right, there are two buttons: "Cancel" and "OK".

**User Name and Password Dialog Box**

3. In the **User Name** text box, type a **valid** Command Software Systems user name.
4. In the **Password** text box, type a **valid** Command Software Systems password.

5. In the **Confirm Password** text box, retype your password, and click **OK**. The system displays the **Updating System** dialog box.



**NOTE:** As some firewalls may have a problem with an active connection, the **Use Passive FTP Connection** check box is selected by default. If the URL specified in the **URL** text box is an FTP URL, the connection is made in passive mode. To use an active connection, clear the **Use Passive FTP Connection** check box.

6. When the installation is complete, the system displays a dialog box informing you that Command Interceptor for MIMESweeper has been successfully installed. Click **Finish**.



**NOTE:** The following services will be started automatically:

- MAILsweeper for SMTP Delivery
  - MAILsweeper for SMTP Receiver
  - MAILsweeper for SMTP Security
7. If you want to schedule updates to the Command Interceptor definition files, go to **Scheduling Command Interceptor Definition File Updates**.  
If you do not, go to **Enabling the Command AntiVirus Scenario**.

## SCHEDULING COMMAND INTERCEPTOR DEFINITION FILE UPDATES



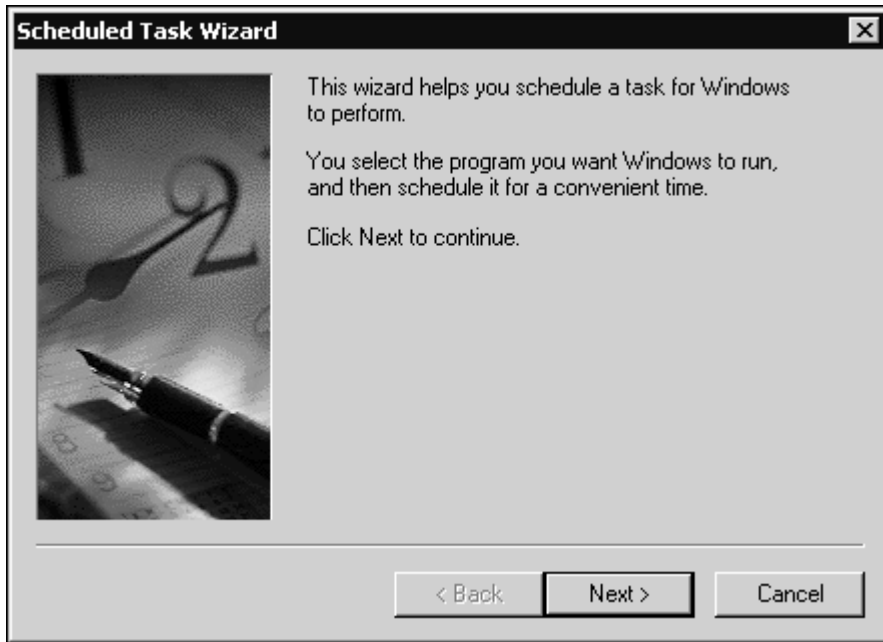
**NOTE:** In Microsoft® Windows for NT® 4.0, you **must** keep at least **one** user logged on for updates to take place successfully.



**NOTE:** You can also update the Command Interceptor definition files manually. For more information, refer to **Updating the Command Interceptor Definition Files Manually**.

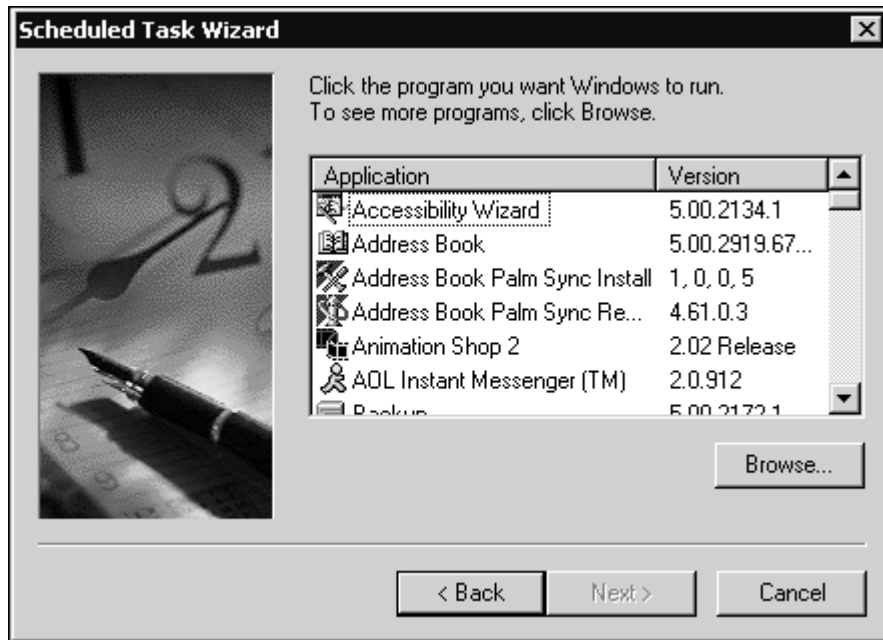
To schedule updates of the Command Interceptor definition files, follow these steps:

1. Open the Windows **Scheduled Task Wizard Main** dialog box:



Scheduled Task Wizard Main Dialog Box

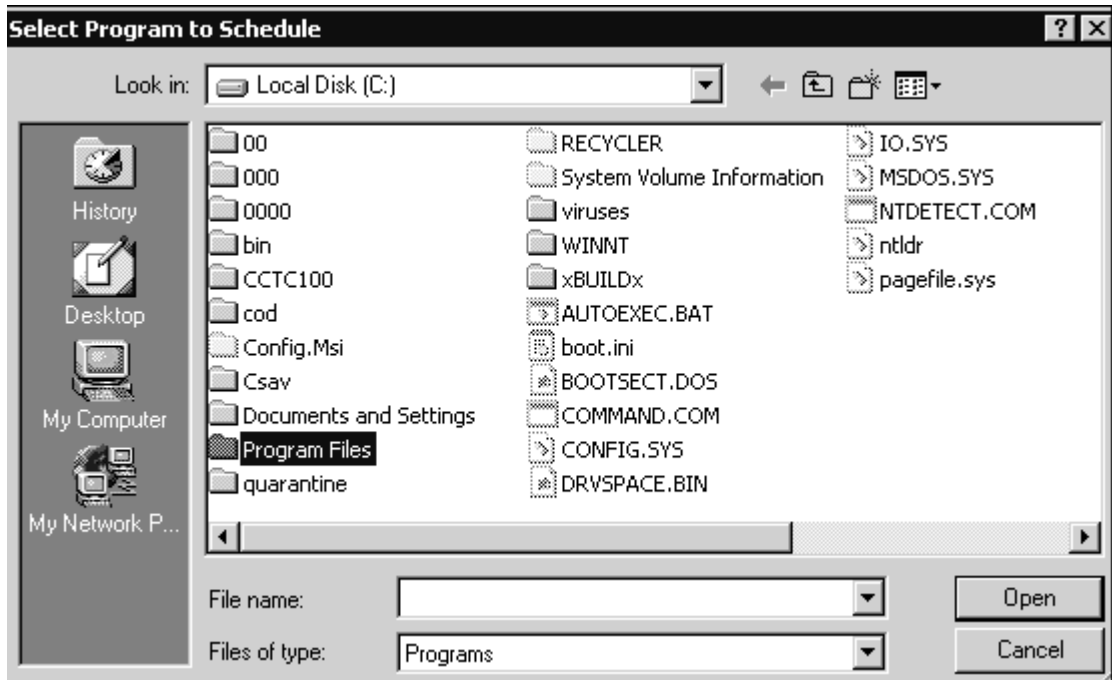
2. Click **Next** to continue. The system displays a **Program Selection** dialog box:



Program Selection Dialog Box

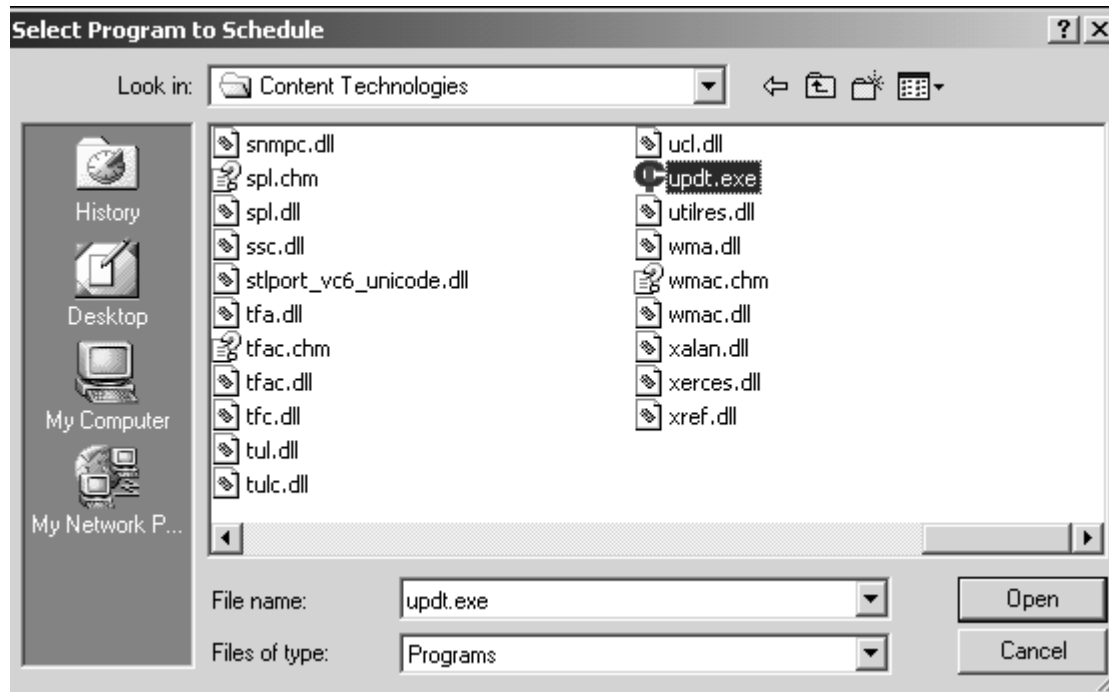
3. Click **Browse**. The system displays the **Select Program to Schedule** dialog box:





Select Program to Schedule Dialog Box

4. Double-click **Program Files**. The system displays the **Program Files** folder.
5. Double-click **Common Files**. The system displays the **Common Files** folder.
6. Double-click **Content Technologies**. The system displays the **Content Technologies** folder:



Select Program to Schedule Dialog Box – Content Technologies Folder

7. Select **updt.exe**, and click **Open**. The system displays a **Task Name and Frequency** dialog box:



**Task Name and Frequency Dialog Box**

8. Select how often you want to perform this task, for example, **Daily**, **Weekly**, **Monthly**, and click **Next**. The system displays a **Time and Day** dialog box:



**Time and Day Dialog Box**

9. In the **Start time** box, select the time of day that you want the update to take place, for example, 1:43 AM.
10. Under **Perform this task**, select the days that you want the update to take place, for example, **Every Day**, **Weekdays**, **Every 5 days**.
11. In the **Start date** box, select the date that you want the updates to start, and click **Next**. The system displays a **User Name and Password** dialog box:



**Scheduled Task Wizard**

Enter the name and password of a user. The task will run as if it were started by that user.

Enter the user name:

Enter the password:

Confirm password:

< Back    Next >    Cancel

**User Name and Password Dialog Box**

12. In the **Enter the user name** text box, type a local user name that has Administrative rights.
  13. In the **Enter the password** text box, type the password of the local user name.
  14. In the **Confirm password** text box, retype the password and click **Next**. The system displays a **Scheduled Task Complete** dialog box:
-



Scheduled Task Complete Dialog Box

15. Click **Finish**.
16. Go to **Enabling the Command AntiVirus Scenario**.

## ENABLING THE COMMAND ANTIVIRUS SCENARIO

To enable the Command AntiVirus Scenario, follow these steps:

1. Open the **MAILsweeper for SMTP Console**.
2. In **Tree** view, locate and right-click **Scenarios**. The system displays a shortcut menu.
3. Select **New**.
4. Select **Scenario**. The system displays a menu containing the available scenarios.
5. On the scenario menu, click **Command AntiVirus**. The system displays the **New Scenario** dialog box.
6. Click **Next**. The system displays the **Options** dialog box.
7. Click **Next**. The system displays the **Format Types** dialog box.
8. Under **Apply to data**, select **Always**.
9. Click **Next**. The system displays the **Location** dialog box.
10. In the **Location** dialog box, you can accept the default location or select a new location under **Browse**.



**NOTE:** If you did not modify the default location during installation, the Command AntiVirus files are copied to:

```
%systemdrive%\Program Files\Common Files\Content Technologies
```

After selecting a location, click **Next**. The system displays the **Clean** dialog box.

11. Choose whether you want to clean (disinfect) detected viruses. If you select **Clean the virus detected**, you have the option of selecting **Annotate cleaned item**.

If you select this option, you can annotate a message in either standard text format or in rich text format. Type the annotation in the text box. Then, use the slider to tell the program to place the annotation at either the start of the e-mail message or at the end of the e-mail message.

When you are finished, click **Next**.

12. Depending on the choices you made in **Step 11**, the systems displays **one** of the following:
  - If you did **not** select **Clean the virus detected** – the system displays an **Infected Classification** dialog box. Select an **Exclusive Classification** from the list and click **Next**. The system displays the **Name** dialog box.
  - If you selected **Clean the virus detected** – the system displays a **Cleaned Classification** dialog box. Select an **Exclusive Classification** from the list and click **Next**. The system displays the **Infected Classification** dialog box. Select an **Exclusive Classification** from the list and click **Next**. The system displays the **Name** dialog box.
13. In the **Name** dialog box, enter a name for the scenario that you are creating and click **Next**. The system displays the **New Scenario** dialog box.
14. Click **Finish** to complete the creation of the scenario.

You can now configure the alerting mechanisms for the classifications listed in the **Classifications** branch.

To configure these mechanisms, follow these steps:

1. Right-click a classification.
2. Select **New** from the shortcut menu.
3. Select **Notification**. The system displays a shortcut menu with the **Alert**, **Inform**, **Log**, and **Reply** options.



4. For details on how to configure these options, see the product's online help or refer to the *MAILsweeper for SMTP Version 4.0 Getting Started Guide*.



**NOTE:** For the customizations to apply, you **must** stop and then start the following services:

- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security

## CREATING A DELETE CLASSIFICATION

This section provides instructions on how to create a classification that deletes infected files that cannot be disinfected.

To create this classification follow these steps:

1. Open the **MAILsweeper for SMTP Console**.
2. In the **Tree** view, locate and right-click **Classifications**. The system displays a shortcut menu.
3. Select **New**.
4. Click **Classification**. The system displays the **New Classification** wizard.
5. Follow the wizard's on-screen instructions to create the new classification. When the system displays the **Name** dialog box, type **Delete** as the name for this new classification.



**NOTE:** Classifications are applied in hierarchical order. After creating the **Delete** classification, you can promote it in the **Classifications** branch so that it is located just beneath the **Cleaned** classification. To promote the **Delete** classification, right-click it and then click **Promote**. This moves the **Delete** classification above the immediately preceding classification. Repeat this process until the **Delete** classification is positioned according to your preferences.



**NOTE:** For the **Delete** classification customization to apply, you **must** stop and then start the following services:

- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security

## UPDATING THE COMMAND INTERCEPTOR DEFINITION FILES MANUALLY

To keep your product's anti-virus abilities up-to-date, please check Command Software System's web site at <http://www.commandsoftware.com/html/defupdate.html>. There, you can download the latest Command Interceptor definition files.

To update the files, follow these steps:



**NOTE:** The following services will be stopped and restarted automatically:

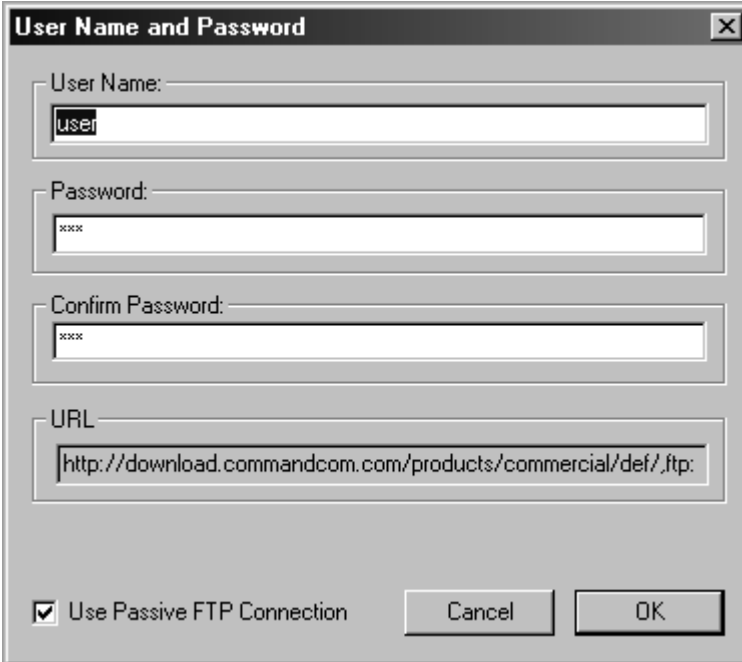
- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security

1. On your system's hard drive, create a temporary folder.
2. Download the file called **DEFINT.MSP** from the Command Software System's web site to the temporary folder that you created in **Step 1**.
3. Double-click the file. This updates the Command Interceptor definition files.
4. Delete the file called **DEFINT.MSP**.

## CHANGING YOUR COMMAND INTERCEPTOR FOR MIMESWEEPER PASSWORD

---

1. Go to the Command Interceptor installation folder.
2. Open the **INTRCEPT** folder, and then double-click the file called **SETUP.EXE**. The system displays the **User Name and Password** dialog box:



The image shows a Windows-style dialog box titled "User Name and Password". It contains four text input fields: "User Name:" with the text "user", "Password:" with "xxxx", "Confirm Password:" with "xxxx", and "URL:" with "http://download.commandcom.com/products/commercial/def/.ftp:". At the bottom, there is a checked checkbox labeled "Use Passive FTP Connection" and two buttons: "Cancel" and "OK".

**User Name and Password Dialog Box**

3. In the **User Name** text box, type a **valid** Command Software Systems user name.
4. In the **Password** text box, type a **valid** Command Software Systems password.

5. In the **Confirm Password** text box, retype your password, and click **OK**. The system displays the **Updating System** dialog box.



**NOTE:** As some firewalls may have a problem with an active connection, the **Use Passive FTP Connection** check box is selected by default. If the URL specified in the **URL** text box is an FTP URL, the connection is made in passive mode. To use an active connection, clear the **Use Passive FTP Connection** check box.

When the installation is complete, the system displays a dialog box informing you that Command Interceptor for MIMESweeper has been successfully installed.

6. Click **Finish**.

## REMOVING COMMAND INTERCEPTOR FOR MIMESWEEPER

To remove the Command Interceptor for MIMESweeper, follow these steps:

1. Open the **MAILsweeper for SMTP Console**.
2. In the **Tree** view, locate and click **Scenarios**.
3. Delete any Command AntiVirus scenarios.
4. Close the **Console**.
5. Using the **Add/Remove Programs** feature in the Windows NT Control Panel, first remove **Command Interceptor for MIMESweeper**.
6. Then, remove the **Command AntiVirus Scenario**.
7. Restart the following services:
  - MAILsweeper for SMTP Delivery
  - MAILsweeper for SMTP Receiver
  - MAILsweeper for SMTP Security



**NOTE:** If you have scheduled updates of the Command Interceptor definition files through the Windows® Scheduled Task Wizard, you also need to delete the scheduled task.

To delete the scheduled task, follow these steps:

1. Click the **Start** button on the Windows taskbar.
2. Select **Settings**.
3. Click **Control Panel**.
4. Double-click **Scheduled Tasks**.
5. Right-click the **UPDT** task. The system displays a drop-down menu.
6. Click **Delete**. The system displays the **Confirm File Delete** dialog box.
7. Click **Yes**.





# MAILSWEEPER 4.1

To enable Command AntiVirus protection, you must install the Command Interceptor™ for MIMESweeper™. The instructions in this chapter can be used to install it from the downloaded file or from the CD.

## PRE-INSTALLATION REQUIREMENTS

---

Before installing the Command Interceptor for MIMESweeper, your system must:

- Be running Windows NT® 4 or higher with Service Pack 4
- Have Microsoft® Internet Explorer 4.01 or higher installed
- Have Microsoft Management Console Version 1.1 installed
- Have MAILsweeper™ 4.1 installed on an NTFS-formatted partition
- Not have any e-mail anti-virus program installed



**NOTE:** To remove a previously installed e-mail anti-virus program, use the **Add/Remove Programs** feature in the Windows NT Control Panel.

If your system does not meet the above-mentioned requirements, Command AntiVirus may not function correctly.

---

## INSTALLING

---

Adding Command AntiVirus to MAILsweeper is a two-step process.

1. Installing the Command Interceptor for MIMESweeper.
2. Enabling the Command AntiVirus Scenario.



**NOTE:** You can also create a Delete classification in MAILsweeper to delete infected files that cannot be disinfected. For more information, refer to **Creating a Delete Classification** located later in this chapter.

## INSTALLING COMMAND INTERCEPTOR FOR MIMESWEEPER

To install the Command Interceptor for MIMESweeper, follow these steps:

1. Open the **MAILsweeper for SMTP Console**.
2. In the **Tree** view, locate and click **Services**.
3. In the left pane, select the following services:
  - MAILsweeper for SMTP Delivery
  - MAILsweeper for SMTP Receiver
  - MAILsweeper for SMTP Security
4. Using the right mouse button (right-click), click the selected service(s), and on the drop-down menu, click **Stop**.
5. If you are installing the Command Interceptor for MIMESweeper from:
  - the downloaded file – go to **Step 6**.
  - the CD – go to **Step 8**.



6. On your system's hard drive, create a temporary folder and move the downloaded file into that folder.
7. Double-click the file. This extracts the Command Interceptor for MIMESweeper files. Go to **Step 9**.
8. Place the CD into the CD drive and change to that drive. Open the folder called MSW4.1x. Then, open the CSAV folder within that folder.
9. Double-click the file called **SETUP.EXE**. The system displays the Welcome screen.
10. Click **Next**. The system displays the Software License Agreement.
11. Click **Yes** to accept the agreement. The system displays the **Start Copying Files** dialog box.
12. Click **Next**. The installation begins, and the system displays the Setup Complete dialog box.
13. Click **Finish**.
14. On your system's hard drive, create a temporary folder.
15. If you are installing the Command Interceptor for MIMESweeper from:
  - the downloaded file, go to the temporary folder that you created in **Step 6**, and copy the file called **M41FXXSE** to the temporary folder that you created in **Step 14**.
  - the CD, open the folder called **MSW4.1x**. Then, open the CSAV folder within that folder. Copy the file called **M41FXXSE** to the temporary folder that you created in **Step 14**.



**NOTE:** The **XX** represents the Command AntiVirus scan engine version number. This number will change with each new release.

16. Double-click the file. This extracts the Command AntiVirus definition files and scan engine.
17. Delete the file called **M41FXXSE**.

18. Copy all of the remaining files to the installation folder. The default is:

```
%systemdrive%\Program Files\Common Files\Content Technologies
```

19. Open the **MAILsweeper for SMTP Console**.

20. In **Tree** view, locate and click **Services**.

21. In the left pane, select the following services:

- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security

22. Right-click the selected service(s), and on the drop-down menu, click **Start**.

23. Go to **Enabling the Command AntiVirus Scenario**.

## ENABLING THE COMMAND ANTIVIRUS SCENARIO

To enable the Command AntiVirus scenario, follow these steps:

1. Open the **MAILsweeper for SMTP Console**.
2. In the left window pane, right-click **Scenarios**. The system displays a shortcut menu.
3. Select **New**.
4. Select **Scenario**. The systems displays a menu containing the available scenarios.
5. On the scenario menu, click **Command AntiVirus**. The system displays the **New Scenario** dialog box.
6. Click **Next**. The system displays the **Options** dialog box.
7. Click **Next**. The system displays the **Format Types** dialog box.
8. Click **Next**. The system displays the **Location** dialog box.
9. In the **Location** dialog box, you can accept the default location or use the **Browse** button to select a new location.



**NOTE:** If you did not modify the default location during installation, the Command AntiVirus files are copied to:

```
%systemdrive%\Program Files\Common Files\Content Technologies
```

After selecting a location, click **Next**. The system displays the **Clean** dialog box.

10. Choose whether you want to clean (disinfect) detected viruses. If you select **Clean the virus detected**, you have the option of selecting **Annotate cleaned message**.

If you select this option, you can annotate a message in either standard text format or in rich text format. Type the annotation in the text box. Then, use the slider to tell the program to place the annotation at either the start of the e-mail message or at the end of the e-mail message.

When you are finished, click **Next**.

11. Depending on the choices you made in **Step 10**, the systems displays one of the following:
  - If you did not select **Clean the virus detected** – the system displays an **Infected Classification** dialog box. Select an **Exclusive Classification** from the list and click **Next**. The system displays the **Name** dialog box.
  - If you selected **Clean the virus detected** – the system displays a **Cleaned Classification** dialog box. Select an **Exclusive Classification** from the list and click **Next**. The system displays the **Infected Classification** dialog box. Select an **Exclusive Classification** from the list and click **Next**. The system displays the **Name** dialog box.
12. In the **Name** dialog box, enter a name for the scenario that you are creating and click **Next**. The system displays the **New Scenario** dialog box.
13. Click **Finish** to complete the creation of the scenario.

Now you can configure the alerting mechanisms for the classifications listed in the **Classifications** branch.

To configure these mechanisms follow these steps:

1. Right-click a classification.
2. Select **New** from the shortcut menu.
3. Select **Notification**. The system displays a shortcut menu with the **Alert**, **Inform**, **Log**, and **Reply** options.
4. For details on how to configure these options, see the product's online help or refer to the *MAILsweeper for SMTP Version 4.0 Getting Started Guide*.



**NOTE:** For the customizations to apply, you **must** stop and then start the following services:

- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security

## CREATING A DELETE CLASSIFICATION

This section provides instructions on how to create a classification that deletes infected files that cannot be disinfected.

To create this classification follow these steps:

1. Open the **MAILsweeper for SMTP Console**.
2. In the left window pane, right-click **Classifications**. The system displays a shortcut menu.
3. Select **New**.
4. Click **Classification**. The system displays the **New Classification** wizard.
5. Follow the wizard's on-screen instructions to create the new classification. When the system displays the **Name** dialog box, type **Delete** as the name for this new classification.



**NOTE:** Classifications are applied in hierarchical order. After creating the **Delete** classification, you can promote it in the **Classifications** branch so that it is located just beneath the **Cleaned** classification. To promote the **Delete** classification, right-click it and then click **Promote**. This moves the **Delete** classification above the immediately preceding classification. Repeat this process until the **Delete** classification is positioned according to your preferences.



**NOTE:** For the **Delete** classification customization to apply, you **must** stop and then start the following services:

- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security

## UPDATING THE COMMAND ANTIVIRUS DEFINITION FILES

To keep your product's anti-virus abilities up-to-date, check Command Software System's web site at <http://www.commandcom.com/html/defupdate.html>. There, you can download the latest Command AntiVirus definition files.

To update the files, follow these steps:



**NOTE:** Before you update the files, you **must** stop the following services:

- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security

1. On your system's hard drive, create a temporary folder.
2. Download the file called **DEFFILES.EXE** from the Command Software System's web site to the temporary folder that you created in **Step 1**.
3. Double-click the file. This extracts the Command AntiVirus definition files.
4. Delete the file called **DEFFILES.EXE**.
5. Copy all of the remaining files to the installation folder. The default is:

`%systemdrive%\Program Files\Common Files\Content Technologies`

6. Restart the following services:
  - MAILsweeper for SMTP Delivery
  - MAILsweeper for SMTP Receiver
  - MAILsweeper for SMTP Security

## REMOVING COMMAND INTERCEPTOR FOR MIMESWEEPER

To remove the Command Interceptor for MIMESweeper, follow these steps:

1. Open the **MAILsweeper for SMTP Console**.
2. In the **Tree** view, locate and click **Scenarios**.
3. Delete any Command AntiVirus scenarios.
4. Close the **Console**.
5. Using the **Add/Remove Programs** feature in the Windows NT Control Panel, remove the **Command AntiVirus Scanner for MIMESweeper**.
6. Restart the following services:
  - MAILsweeper for SMTP Delivery
  - MAILsweeper for SMTP Receiver
  - MAILsweeper for SMTP Security

# MAILSWEEPER 4.0



To enable Command AntiVirus protection, you must install the Command Interceptor™ for MIMESweeper™. The instructions in this chapter can be used to install it from the downloaded file or from the CD.

## PRE-INSTALLATION REQUIREMENTS

---

Before installing the Command Interceptor for MIMESweeper, your system must:

- Be running Windows NT® 4 or higher with Service Pack 4
- Have Microsoft® Internet Explorer 4.01 or higher installed
- Have Microsoft Management Console Version 1.1 installed
- Have MAILsweeper™ 4.0 installed on an NTFS-formatted partition
- Not have any e-mail anti-virus program installed



**NOTE:** To remove a previously installed e-mail antivirus program, use the **Add/Remove Programs** feature in the Windows NT Control Panel.

If your system does not meet the above-mentioned requirements, Command AntiVirus may not function correctly.

---

## INSTALLING

---

Adding Command AntiVirus to MAILsweeper is a two-step process.

1. Installing the Command Interceptor for MIMESweeper.
2. Enabling the Command AntiVirus Scenario.



**NOTE:** You can also create a Delete classification in MAILsweeper to delete infected files that cannot be disinfected. For more information, refer to **Creating a Delete Classification** located later in this chapter.

## INSTALLING COMMAND INTERCEPTOR FOR MIMESWEEPER

To install the Command Interceptor for MIMESweeper, follow these steps:

1. Open the **MAILsweeper for SMTP Console**.
2. In the **Tree** view, locate and click **Services**.
3. In the left pane, select the following services:
  - MAILsweeper for SMTP Delivery
  - MAILsweeper for SMTP Receiver
  - MAILsweeper for SMTP Security
4. Using the right mouse button (right-click), click the selected service(s), and on the drop-down menu, click **Stop**.
5. If you are installing the Command Interceptor for MIMESweeper from:
  - the downloaded file – go to **Step 6**.
  - the CD – go to **Step 8**.



6. On your system's hard drive, create a temporary folder and move the downloaded file into that folder.
7. Double-click the file. This extracts the Command Interceptor for MIMESweeper files. Go to **Step 9**.
8. Place the CD into the CD drive and change to that drive. Open the folder called MSW4.0x. Then, open the CSAV folder within that folder.
9. Double-click the file called **SETUP.EXE**. The system displays the Welcome screen.
10. Click **Next**. The system displays the Software License Agreement.
11. Click **Yes** to accept the agreement. The system displays the **Start Copying Files** dialog box.
12. Click **Next**. The installation begins and the system displays the **Setup Complete** dialog box.
13. Click **Finish**.
14. Open the **MAILsweeper for SMTP Console**.
15. In **Tree** view, locate and click **Services**.
16. In the left pane, select the following services:
  - MAILsweeper for SMTP Delivery
  - MAILsweeper for SMTP Receiver
  - MAILsweeper for SMTP Security
17. Right-click the selected service(s), and on the drop-down menu, click **Start**.
18. Go to **Enabling the Command AntiVirus Scenario**.

## ENABLING THE COMMAND ANTIVIRUS SCENARIO

To enable the Command AntiVirus scenario, follow these steps:

1. Open the **MAILsweeper for SMTP Console**.
2. In the left window pane, right-click **Scenarios**. The system displays a shortcut menu.
3. Select **New**.
4. Select **Scenario**. The systems displays a menu containing the available scenarios.
5. On the scenario menu, click **Command AntiVirus**. The system displays the **New Scenario** dialog box.
6. Click **Next**. The system displays the **Options** dialog box.
7. Click **Next**. The system displays the **Format Types** dialog box.
8. Click **Next**. The system displays the **Location** dialog box.
9. In the **Location** dialog box, you can accept the default location or use the **Browse** button to select a new location.



**NOTE:** If you did not modify the default location during installation, the Command AntiVirus files are copied to:

```
%systemdrive%\Program Files\Common Files\Content Technologies
```

After selecting a location, click **Next**. The system displays the **Clean** dialog box.

10. Choose whether you want to clean (disinfect) detected viruses. If you select **Clean the virus detected**, you have the option of selecting **Annotate cleaned message**.

If you select this option, you can annotate a message in either standard text format or in rich text format. Type the annotation in the text box. Then, use the slider to tell the program to place the annotation at either the start of the e-mail message or at the end of the e-mail message.

When you are finished, click **Next**.

11. Depending on the choices you made in **Step 10**, the system displays one of the following:
  - If you did **not** select **Clean the virus detected** – the system displays an **Infected Classification** dialog box. Select an **Exclusive Classification** from the list and click **Next**. The system displays the **Name** dialog box.
  - If you selected **Clean the virus detected** – the system displays a **Cleaned Classification** dialog box. Select an **Exclusive Classification** from the list and click **Next**. The system displays the **Infected Classification** dialog box. Select an **Exclusive Classification** from the list and click **Next**. The system displays the **Name** dialog box.
12. In the **Name** dialog box, enter a name for the scenario that you are creating and click **Next**. The system displays the **New Scenario** dialog box.
13. Click **Finish** to complete the creation of the scenario.

Now you can configure the alerting mechanisms for the classifications listed in the **Classifications** branch.

To configure these mechanisms follow these steps:

1. Right-click a classification.
2. Select **New** from the shortcut menu.
3. Select **Notification**. The system displays a shortcut menu with the **Alert**, **Inform**, **Log**, and **Reply** options.
4. For details on how to configure these options, see the product's online help or refer to the *MAILsweeper for SMTP Version 4.0 Getting Started Guide*.



**NOTE:** For the customizations to apply, you **must** stop and then start the following services:

- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security

## CREATING A DELETE CLASSIFICATION

This section provides instructions on how to create a classification that deletes infected files that cannot be disinfected.

To create this classification follow these steps:

1. Open the **MAILsweeper for SMTP Console**.
2. In the left window pane, right-click **Classifications**. The system displays a shortcut menu.
3. Select **New**.
4. Click **Classification**. The system displays the **New Classification** wizard.
5. Follow the wizard's on-screen instructions to create the new classification. When the system displays the **Name** dialog box, type **Delete** as the name for this new classification.



**NOTE:** Classifications are applied in hierarchical order. After creating the **Delete** classification, you can promote it in the **Classifications** branch so that it is located just beneath the **Cleaned** classification. To promote the **Delete** classification, right-click it and then click **Promote**. This moves the **Delete** classification above the immediately preceding classification. Repeat this process until the **Delete** classification is positioned according to your preferences.



**NOTE:** For the **Delete** classification customization to apply, you **must** stop and then start the following services:

- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security

## UPDATING THE COMMAND ANTIVIRUS DEFINITION FILES

To keep your product's anti-virus abilities up-to-date, please check Command Software System's web site at <http://www.commandcom.com/html/defupdate.html>. There, you can download the latest Command AntiVirus definition files.

To update the files, follow these steps:



**NOTE:** Before you update the files, you **must** stop the following services:

- MAILsweeper for SMTP Delivery
- MAILsweeper for SMTP Receiver
- MAILsweeper for SMTP Security

1. On your system's hard drive, create a temporary folder.
2. Download the file called **DEFFILES.EXE** from the Command Software System's web site to the temporary folder that you created in **Step 1**.
3. Double-click the file. This extracts the Command AntiVirus definition files.
4. Delete the file called **DEFFILES.EXE**.
5. Copy all of the remaining files to the installation folder. The default is:

`%systemdrive%\Program Files\Common Files\Content Technologies`

6. Restart the following services:
  - MAILsweeper for SMTP Delivery
  - MAILsweeper for SMTP Receiver
  - MAILsweeper for SMTP Security

## REMOVING COMMAND INTERCEPTOR FOR MIMESWEEPER

To remove the Command Interceptor for MIMESweeper, follow these steps:

1. Open the **MAILsweeper for SMTP Console**.
2. In the **Tree** view, locate and click **Scenarios**.
3. Delete any Command AntiVirus scenarios.
4. Close the **Console**.
5. Using the **Add/Remove Programs** feature in the Windows NT Control Panel, remove the **Command AntiVirus Scanner**.
6. Restart the following services:
  - MAILsweeper for SMTP Delivery
  - MAILsweeper for SMTP Receiver
  - MAILsweeper for SMTP Security



# MAILSWEEPER 3.2

To enable Command AntiVirus protection, you must install the Command Interceptor™ for MIMESweeper™. The instructions in this chapter can be used to install it from the downloaded file or from the CD.

## PRE-INSTALLATION REQUIREMENTS

---

Before installing the Command Interceptor for MIMESweeper, your system must:

- Have MAILsweeper™ 3.2 installed
- Not have any e-mail anti-virus program installed



**NOTE:** To remove a previously installed e-mail anti-virus program, use the **Add/Remove Programs** feature in the Windows NT® Control Panel.

If your system does not meet the above-mentioned requirements, Command AntiVirus may not function correctly.

---

## INSTALLING

---

To install the Command Interceptor for MIMESweeper, follow these steps:

1. Stop all Services.
2. Make a copy of the **VALIDATE.CFG** file and save it as a backup file. This file is located in the **CONFIG** folder of the MIMESweeper program folder.
3. Using Notepad, open the **VALIDATE.CFG** file.
4. Go to the **Validation Configuration Section**.
5. Remove from and including **[Validation]** to and excluding **[DetectJava=]**.
6. Copy and paste in the same place the following:

```
[ VALIDATION ]
CSAVDLL=CMDAV

HTML=VALHTML
VALIDATEATTRIBUTES=VALATTR

[ CSAVDLL ]
PERFORMIF=CONTAINERCLASS==EXECUTABLE
PERFORMIF=CONTAINERCLASS==DOCUMENT
PERFORMIF=CONTAINERCLASS==TEXT
PERFORMIF=CONTAINERCLASS==BINARY

0=SUCCESS
1=VIRUSPRESENT
255=SCANFAILED
```

7. Save and close the file.
8. Click the **Start** button.
9. Click **Run**.
10. In the **Open** text box, type **regedit**.
11. Click **OK**.



12. Click the plus sign (+) to the left of **HKEY\_LOCAL\_MACHINE**.
13. Click the plus sign (+) to the left of **SOFTWARE**.
14. Click the plus sign (+) to the left of **Content Technologies**.
15. Click the plus sign (+) to the left of **MIMESweeper**.
16. Select **MIMESweeper**.
17. In an empty space in the right pane, click the right mouse button (right-click).
18. Click **New**.
19. Click **String Value**.
20. In the text box, type Location
21. Press **Enter**.
22. Select **Location**, and right-click.
23. Click **Modify**.
24. Enter the path of the MIMESweeper installation folder, for example:

```
C:\MSW\PROGRAM
```

25. Click **OK**. The added line in the registry should read:

```
LOCATION          "C:\\MSW\\PROGRAM"
```

26. If you are using the electronic version of the Command Interceptor for MIMESweeper, extract and copy the CSAV files into the MIMESweeper program folder that you specified in **Step 24**.  
  
If you are using the CD version, copy the Command Interceptor for MIMESweeper files from the MSW3.2x\CSAV folder into the MIMESweeper program folder that you specified in **Step 24**.
  27. Restart the Server and or Services.
-

## REMOVING COMMAND INTERCEPTOR FOR MIMESWEEPER

To remove Command Interceptor for MIMESweeper, remove the lines that you added to the **Validation Configuration Section** of the **VALIDATE.CFG** file. For more information, refer to **Installing** located previously in this chapter.



# WEBSWEEPER 4.X

To enable Command Interceptor protection, you must install the Command AntiVirus Scenario for WEBSweeper™ and the Command Interceptor™ for MIMESweeper™. The instructions in this chapter can be used to install them from the downloaded file or from the CD.

## PRE-INSTALLATION REQUIREMENTS

---

Before installing the Command Interceptor for MIMESweeper, your system must:

- Have WEBSweeper 4.0 or 4.1 installed on an NTFS-formatted partition
- Not have any e-mail anti-virus program installed



**NOTE:** To remove a previously installed e-mail anti-virus program, use the **Add/Remove Programs** feature in the Windows NT® Control Panel.

If your system does not meet the above-mentioned requirements, Command Interceptor may not function correctly.

---

## INSTALLING

---

Adding Command Interceptor to WEBSweeper is a four-step process.

1. Installing the Command AntiVirus Scenario.
2. Installing the Command Interceptor for MIMESweeper.
3. Scheduling Command Interceptor Definition File Updates
4. Enabling the Command AntiVirus Scenario.



**NOTE:** You can also create a Delete classification in WEBSweeper to delete infected files that cannot be disinfected. For more information, refer to **Creating a Delete Classification** located later in this chapter.

## INSTALLING THE COMMAND ANTIVIRUS SCENARIO

To install the Command AntiVirus Scenario, follow these steps:

1. Open the **WEBSweeper Console**.
2. In the **Tree** view, locate and click **Services**.
3. In the left pane, select the **WEBSweeper Security** service.
4. Using the right mouse button (right-click), click the selected service, and on the drop-down menu, click **Stop**.
5. If you are installing the Command AntiVirus Scenario from:
  - **the downloaded file** – On your system's hard drive, create a Command Interceptor installation folder. Move the downloaded file to this folder. Then, double-click the file. This extracts the Command Interceptor files. Go to **Step 6**.
  - **the CD** – Place the CD into the CD-ROM drive and change to that drive. Open the folder called **MSW4.2x**. Go to **Step 6**.
6. Open the **WEBSCEN** folder, and then double-click the file called **SETUP.EXE**. The system displays a **Welcome** screen.

7. Click **Next** to continue. Follow the instructions in the dialog boxes.
8. When the installation is complete, go to **Installing Command Interceptor for MIMESweeper**.

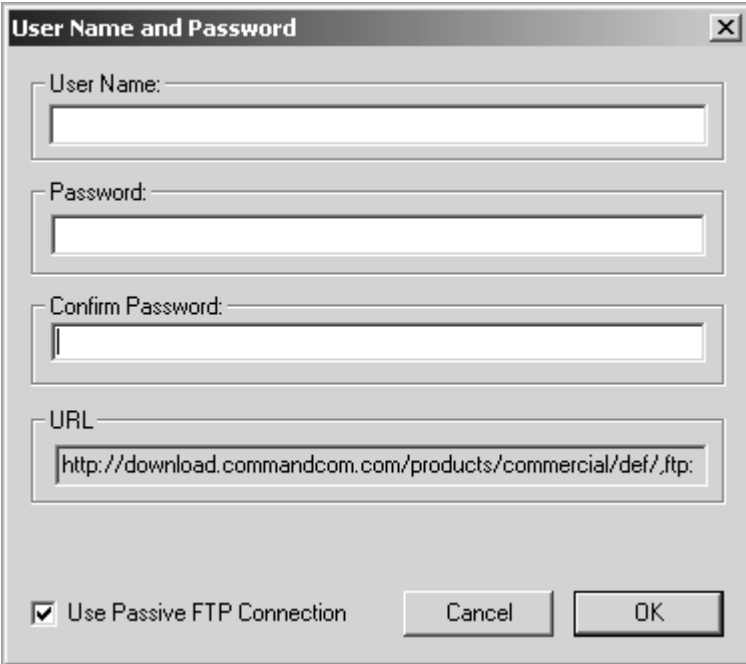
## INSTALLING COMMAND INTERCEPTOR FOR MIMESWEEPER

1. If you are installing the Command Interceptor for MIMESweeper from:
  - **the downloaded file** – go to the Command Interceptor installation folder that you created in **Step 5 of Installing the Command AntiVirus Scenario**, and open that folder. Then go to **Step 2**.
  - **the CD** – place the CD into the CD-ROM drive and change to that drive. Open the folder called **MSW4.2x**. Go to **Step 2**.
2. Open the **INTRCEPT** folder, and then double-click the file called **SETUP.EXE**. The system displays the **User Name and Password** dialog box.



**NOTE: Experienced Users Only** - You can also start the installation program by running the **msiexec** with the following parameters:

```
msiexec /i intrcept.msi REINSTALL=ALL REINSTALLMODE=vomus
```



The image shows a dialog box titled "User Name and Password" with a close button (X) in the top right corner. It contains four text input fields: "User Name:", "Password:", "Confirm Password:", and "URL:". The "URL:" field contains the text "http://download.commandcom.com/products/commercial/def/.ftp:". At the bottom left, there is a checked checkbox labeled "Use Passive FTP Connection". At the bottom right, there are two buttons: "Cancel" and "OK".

**User Name and Password Dialog Box**

3. In the **User Name** text box, type a **valid** Command Software Systems user name.
4. In the **Password** text box, type a **valid** Command Software Systems password.

5. In the **Confirm Password** text box, retype your password, and click **OK**. The system displays the **Updating System** dialog box.



**NOTE:** As some firewalls may have a problem with an active connection, the **Use Passive FTP Connection** check box is selected by default. If the URL specified in the **URL** text box is an FTP URL, the connection is made in passive mode. To use an active connection, clear the **Use Passive FTP Connection** check box.

6. When the installation is complete, the system displays a dialog box informing you that Command Interceptor for MIMESweeper has been successfully installed. Click **Finish**.



**NOTE:** The **WEBSweeper Security** service will be started automatically.

7. If you want to schedule updates to the Command Interceptor definition files, go to **Scheduling Command Interceptor Definition File Updates**.

If you do not, go to **Enabling the Command AntiVirus Scenario**.

## SCHEDULING COMMAND INTERCEPTOR DEFINITION FILE UPDATES



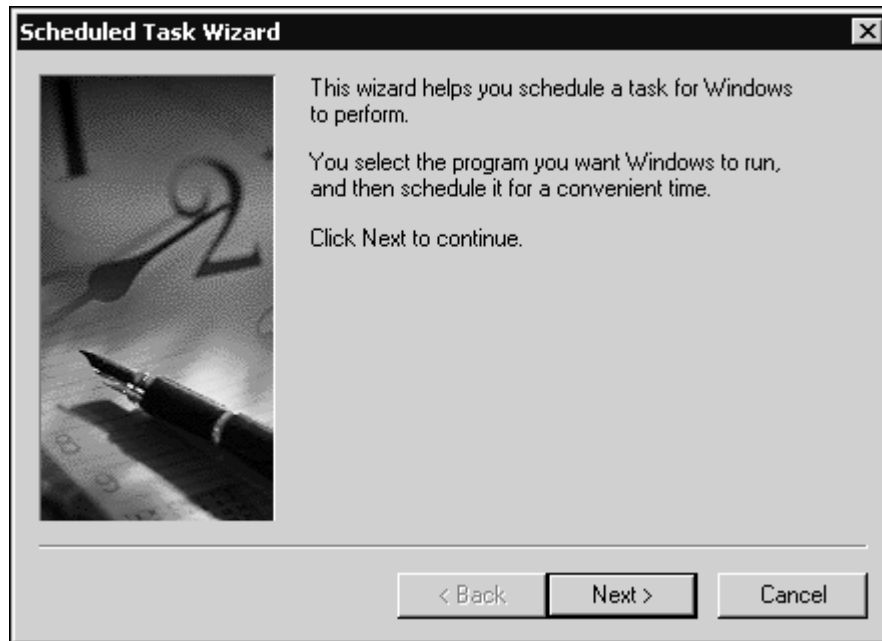
**NOTE:** In Microsoft® Windows for NT® 4.0, you **must** keep at least **one** user logged on for updates to take place successfully.



**NOTE:** You can also update the Command Interceptor definition files manually. For more information, refer to **Updating the Command Interceptor Definition Files Manually**.

To schedule updates of the Command Interceptor definition files, follow these steps:

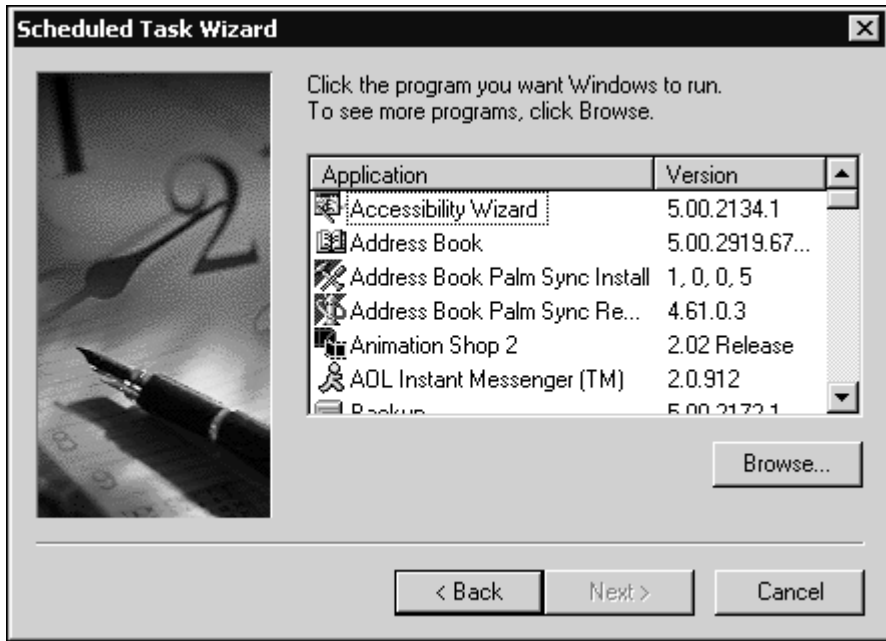
1. Open the Windows **Scheduled Task Wizard Main** dialog box:



**Scheduled Task Wizard Main Dialog Box**

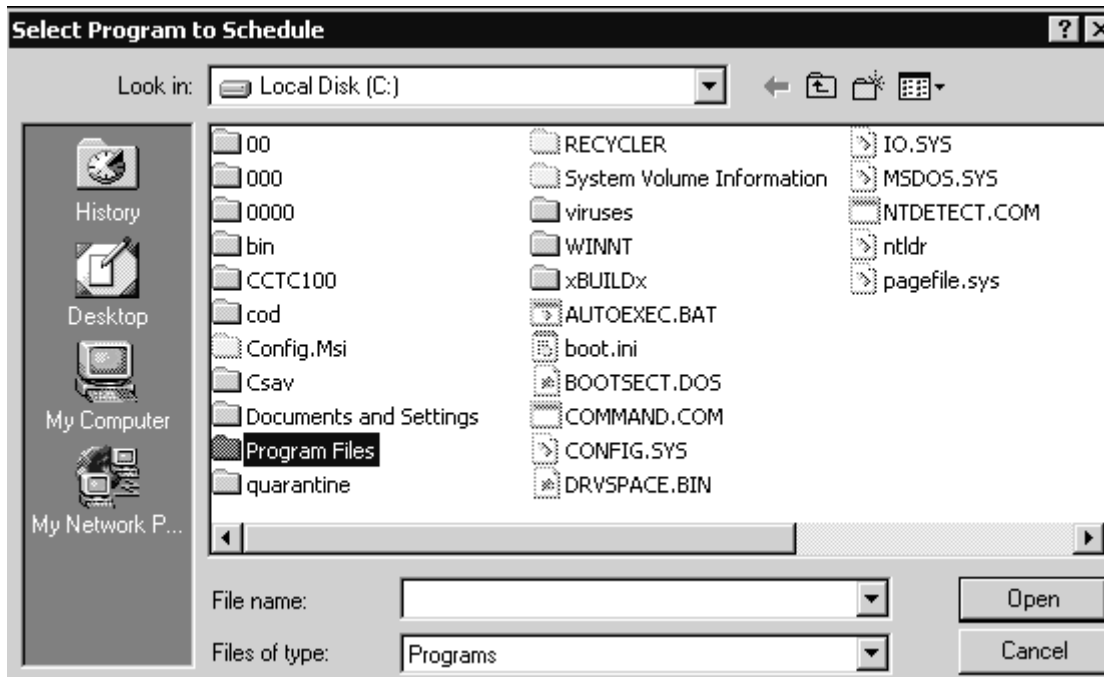
2. Click **Next** to continue. The system displays a **Program Selection** dialog box:





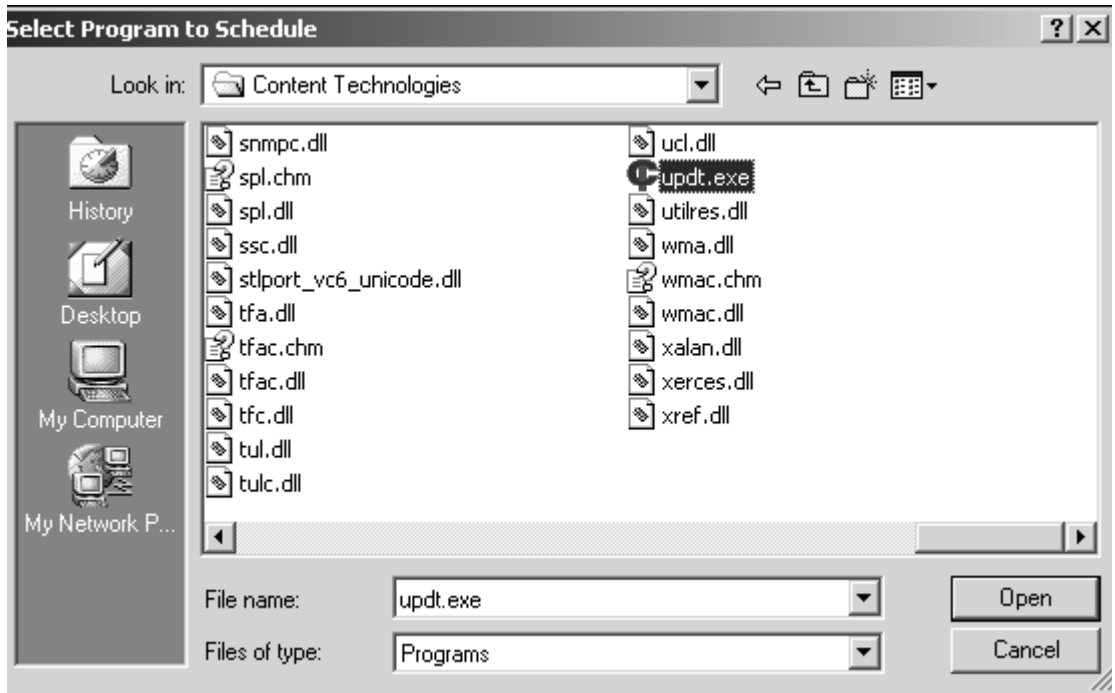
Program Selection Dialog Box

3. Click **Browse**. The system displays the **Select Program to Schedule** dialog box:



Select Program to Schedule Dialog Box

4. Double-click **Program Files**. The system displays the **Program Files** folder.
5. Double-click **Common Files**. The system displays the **Common Files** folder.
6. Double-click **Content Technologies**. The system displays the **Content Technologies** folder:



Select Program to Schedule Dialog Box – Content Technologies Folder

7. Select **updt.exe**, and click **Open**. The system displays a **Task Name and Frequency** dialog box:



**Task Name and Frequency Dialog Box**

8. Select how often you want to perform this task, for example, **Daily**, **Weekly**, **Monthly**, and click **Next**. The system displays a **Time and Day** dialog box:



Time and Day Dialog Box

9. In the **Start time** box, select the time of day that you want the update to take place, for example, 1:43 AM.
10. Under **Perform this task**, select the days that you want the update to take place, for example, **Every Day**, **Weekdays**, **Every 5 days**.
11. In the **Start date** box, select the date that you want the updates to start, and click **Next**. The system displays a **User Name and Password** dialog box:



**Scheduled Task Wizard**

Enter the name and password of a user. The task will run as if it were started by that user.

Enter the user name:

Enter the password:

Confirm password:

< Back    Next >    Cancel

**User Name and Password Dialog Box**

12. In the **Enter the user name** text box, type a local user name that has Administrative rights.
13. In the **Enter the password** text box, type the password of the local user name.
14. In the **Confirm password** text box, retype the password and click **Next**. The system displays a **Scheduled Task Complete** dialog box:



Scheduled Task Complete Dialog Box

15. Click **Finish**.
16. Go to **Enabling the Command AntiVirus Scenario**.

## ENABLING THE COMMAND ANTIVIRUS SCENARIO

To enable the Command AntiVirus Scenario, follow these steps:

1. Open the **WEBSweeper Console**.
2. In **Tree** view, locate and right-click **Scenarios**. The system displays a shortcut menu.
3. Select **New**.
4. Select **Scenario**. The system displays a menu containing the available scenarios.
5. On the scenario menu, click **Command AntiVirus**. The system displays the **New Scenario** dialog box.
6. Click **Next**. The system displays the **Options** dialog box.
7. Click **Next**. The system displays the **Format Types** dialog box.
8. Under **Apply to data**, select **Always**.
9. Click **Next**. The system displays the **Location** dialog box.
10. In the **Location** dialog box, you can accept the default location or select a new location under **Browse**.



**NOTE:** If you did not modify the default location during installation, the Command AntiVirus files are copied to:

```
%systemdrive%\Program Files\Common Files\Content Technologies
```

After selecting a location, click **Next**. The system displays the **Clean** dialog box.

11. Choose whether you want to clean (disinfect) detected viruses. If you select **Clean the virus detected**, you have the option of selecting **Annotate cleaned item**.

If you select this option, you can annotate a message in either standard text format or in rich text format. Type the annotation in the text box. Then, use the slider to tell the program to place the annotation at either the start of the e-mail message or at the end of the e-mail message.

When you are finished, click **Next**.



12. Depending on the choices you made in **Step 11**, the system displays **one** of the following:
  - If you did **not** select **Clean the virus detected** – the system displays an **Infected Classification** dialog box. Select an **Exclusive Classification** from the list and click **Next**. The system displays the **Name** dialog box.
  - If you selected **Clean the virus detected** – the system displays a **Cleaned Classification** dialog box. Select an **Exclusive Classification** from the list and click **Next**. The system displays the **Infected Classification** dialog box. Select an **Exclusive Classification** from the list and click **Next**. The system displays the **Name** dialog box.
13. In the **Name** dialog box, enter a name for the scenario that you are creating and click **Next**. The system displays the **New Scenario** dialog box.
14. Click **Finish** to complete the creation of the scenario.

You can now configure the alerting mechanisms for the classifications listed in the **Classifications** branch.

To configure these mechanisms:

1. Right-click a classification.
2. Select **New** from the shortcut menu.
3. Select **Notification**. The system displays a shortcut menu with the **Alert**, **Inform**, **Log**, and **Reply** options.
4. For details on how to configure these options, see the product's online help or refer to the *WEBSweeper for 4.0 Administrator's Guide*.



**NOTE:** For the customizations to apply, you **must** stop and then start the **WEBSweeper Security** service.

## CREATING A DELETE CLASSIFICATION

This section provides instructions on how to create a classification that deletes infected files that cannot be disinfected.

To create this classification follow these steps:

1. Open the **WEBSweeper Console**.
2. In the **Tree** view, locate and right-click **Classifications**. The system displays a shortcut menu.
3. Select **New**.
4. Click **Classification**. The system displays the **New Classification** wizard.
5. Follow the wizard's on-screen instructions to create the new classification. When the system displays the **Name** dialog box, type **Delete** as the name for this new classification.



**NOTE:** Classifications are applied in hierarchical order. After creating the **Delete** classification, you can promote it in the **Classifications** branch so that it is located just beneath the **Cleaned** classification. To promote the **Delete** classification, right-click it and then click **Promote**. This moves the **Delete** classification above the immediately preceding classification. Repeat this process until the **Delete** classification is positioned according to your preferences.



**NOTE:** For the **Delete** classification customization to apply, you **must** stop and then start the **WEBSweeper Security** service.

## UPDATING THE COMMAND INTERCEPTOR DEFINITION FILES MANUALLY

To keep your product's anti-virus abilities up-to-date, please check Command Software System's web site at <http://www.commandsoftware.com/html/defupdate.html>. There, you can download the latest Command Interceptor definition files.

To update the files, follow these steps:



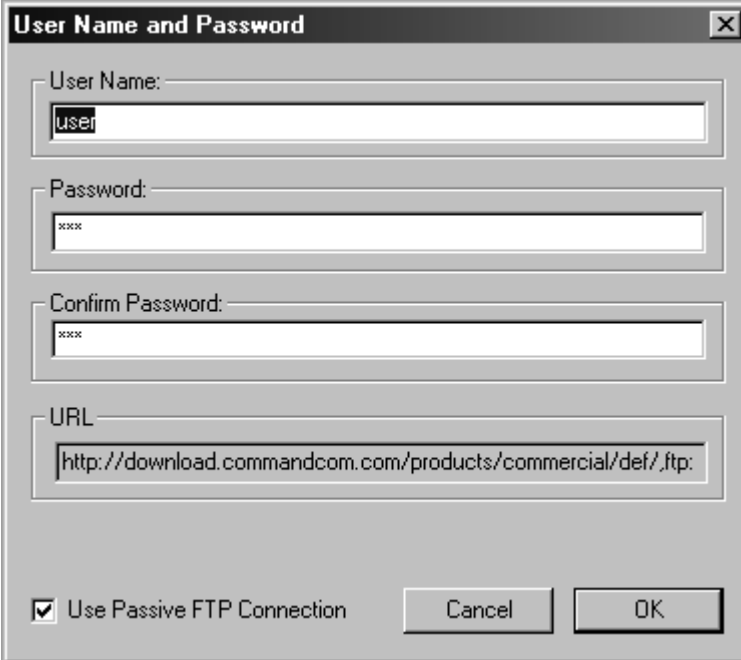
**NOTE:** The **WEBSweeper Security** service will be stopped and restarted automatically.

1. On your system's hard drive, create a temporary folder.
2. Download the file called **DEFINT.MSP** from the Command Software System's web site to the temporary folder that you created in **Step 1**.
3. Double-click the file. This updates the Command Interceptor definition files.
4. Delete the file called **DEFINT.MSP**.

## CHANGING YOUR COMMAND INTERCEPTOR FOR MIMESWEEPER PASSWORD

---

1. Go to the Command Interceptor installation folder.
2. Open the **INTRCEPT** folder, and then double-click the file called **SETUP.EXE**. The system displays the **User Name and Password** dialog box:



The image shows a Windows-style dialog box titled "User Name and Password". It contains four text input fields: "User Name:" with the text "User", "Password:" with "xxx", "Confirm Password:" with "xxx", and "URL:" with "http://download.commandcom.com/products/commercial/def/,ftp:". At the bottom, there is a checked checkbox labeled "Use Passive FTP Connection" and two buttons: "Cancel" and "OK".

**User Name and Password Dialog Box**

3. In the **User Name** text box, type a **valid** Command Software Systems user name.
4. In the **Password** text box, type a **valid** Command Software Systems password.

5. In the **Confirm Password** text box, retype your password, and click **OK**. The system displays the **Updating System** dialog box.



**NOTE:** As some firewalls may have a problem with an active connection, the **Use Passive FTP Connection** check box is selected by default. If the URL specified in the **URL** text box is an FTP URL, the connection is made in passive mode. To use an active connection, clear the **Use Passive FTP Connection** check box.

When the installation is complete, the system displays a dialog box informing you that Command Interceptor for MIMESweeper has been successfully installed.

6. Click **Finish**.

## REMOVING COMMAND INTERCEPTOR FOR MIMESWEEPER

To remove the Command Interceptor for MIMESweeper, follow these steps:

1. Open the **WEBSweeper Console**.
2. In the **Tree** view, locate and click **Scenarios**.
3. Delete any Command AntiVirus scenarios.
4. Close the **Console**.
5. Using the **Add/Remove Programs** feature in the Windows NT Control Panel, first remove **Command Interceptor for MIMESweeper**.
6. Then, remove the **Command AntiVirus Scenario**.
7. Restart the **WEBSweeper Security** service.



**NOTE:** If you have scheduled updates of the Command Interceptor definition files through the Windows® Scheduled Task Wizard, you also need to delete the scheduled task.

To delete the scheduled task, follow these steps:

1. Click the **Start** button on the Windows taskbar.
2. Select **Settings**.
3. Click **Control Panel**.
4. Double-click **Scheduled Tasks**.
5. Right-click the **UPDT** task. The system displays a drop-down menu.
6. Click **Delete**. The system displays the **Confirm File Delete** dialog box.
7. Click **Yes**.