# Command On Demand™

## User's Guide

# NOTICE

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

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

# LICENSE AGREEMENT

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

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

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

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

# WARRANTY

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

**Command AntiVirus © Copyright 2000 by Command Software Systems, Inc.
Portions © Copyright 1993, 2000 FRISK Software International.**

**Published in the U.S.A. by Command Software Systems, Inc. All rights reserved.**
**Document No. COD-14-0701**

**Part No. 07-2101-00**

# TABLE OF CONTENTS


**INTRODUCTION ..... 1-1**

Main Features ..... 1-1
Chapter Overview ..... 1-2
- Chapter 1 - Introduction ..... 1-2
- Chapter 2 - Using Command On Demand ..... 1-2
- Chapter 3 - Glossary ..... 1-2

Conventions Used ..... 1-3
System Requirements ..... 1-4

**USING COMMAND ON DEMAND ..... 2-1**

Getting Started ..... 2-1
- Internet Explorer ..... 2-2
- Netscape ..... 2-5

The Command On Demand Main Dialog Box ..... 2-19
- Components ..... 2-20

Using Command On Demand Main Dialog Box ..... 2-22
- Starting a Scan ..... 2-22
- Stopping a Scan ..... 2-23
- Disinfecting Infected Files ..... 2-24

On-access Protection ..... 2-25
- Documentation Files ..... 2-25
- Downloading ..... 2-27
- E-mail Messages ..... 2-29

Troubleshooting ..... 2-31
- Failure to Install ..... 2-31
- Incompatible Version ..... 2-33

Removing Command On Demand ..... 2-33

**GLOSSARY ..... 3-1**

# INTRODUCTION

Command On Demand™ is an on-demand anti-virus scanner for web users that provides the latest technology for preventing the spread of computer viruses. Command On Demand is easy to use. Just select a file or folder and click **Scan** to detect and disinfect any virus-infected files.

**NOTE:** If you are using the **Biz Dev** version of Command On Demand, the disinfection feature is **not** available.

## MAIN FEATURES

Command On Demand is a comprehensive anti-virus protection program that:

- Uses state-of-the-art technology to scan for thousands of known viruses and their variants.
- Scans hard drives, diskettes, CD-ROMs, network drives, directories, and specific files.
- Scans for macro viruses and Trojan Horses.
- Scans compressed files and compressed executables.
- Removes viruses without damaging the original file.
- Safely removes viruses from files.

**NOTE:** If you are using the Virus Striker version of Command On Demand, it also contains the Command Module™ for Office plugin. Through this plugin, Virus Striker also provides on-access scanning for web users that provides the latest anti-virus technology for Microsoft® Office 2000 and Microsoft® Internet Explorer 5.x or higher.

For example, Virus Striker:

- Automatically scans and disinfects files opened in Microsoft Word, Power Point, and Excel in Office 2000.
- Automatically scans and disinfects files downloaded through Internet Component Download (ICD) in Microsoft Internet Explorer Version 5.x.
- Automatically scans and disinfects the body and attachments of all messages sent and received while you are logged into Microsoft Exchange client or Microsoft Outlook.

# CHAPTER OVERVIEW

The *Command On Demand User's Guide* consists of the following chapters:

## CHAPTER 1 - INTRODUCTION

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

## CHAPTER 2 - USING COMMAND ON DEMAND

This chapter provides instructions on how to perform an anti-virus scan of your drives and folders. Chapter 2 also includes information on the components of the Command On Demand Graphical User Interface (GUI) or **Command On Demand Main** dialog box.

## CHAPTER 3 - GLOSSARY

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

# CONVENTIONS USED

Indicates an area that requires special attention.

Indicates a helpful tip.

Indicates network-specific information.

Indicates a task that requires administrator rights to perform.

Indicates information that is specific to the server version of Command AntiVirus.

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

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

**CSAV** The acronym used for Command AntiVirus

# SYSTEM REQUIREMENTS

### Client

To operate Command On Demand, you must have Windows® 9x, Windows Me, or Windows NT/2000 installed with Microsoft® Internet Explorer Version 4.0 or higher, or Netscape® Communicator Version 4.6 or higher.

# USING COMMAND ON DEMAND

Command On Demand™ provides an easy and effective way to scan for viruses. This chapter provides information on getting started. It also covers how to use Command On Demand to scan your drives and folders for viruses.

**NOTE:** For customers using the Virus Striker version of Command On Demand, this chapter also contains information on the on-access protection provided for Microsoft® Office 2000 and Microsoft Internet Explorer through the Command Module™ for Office (CMO) plugin.

## GETTING STARTED

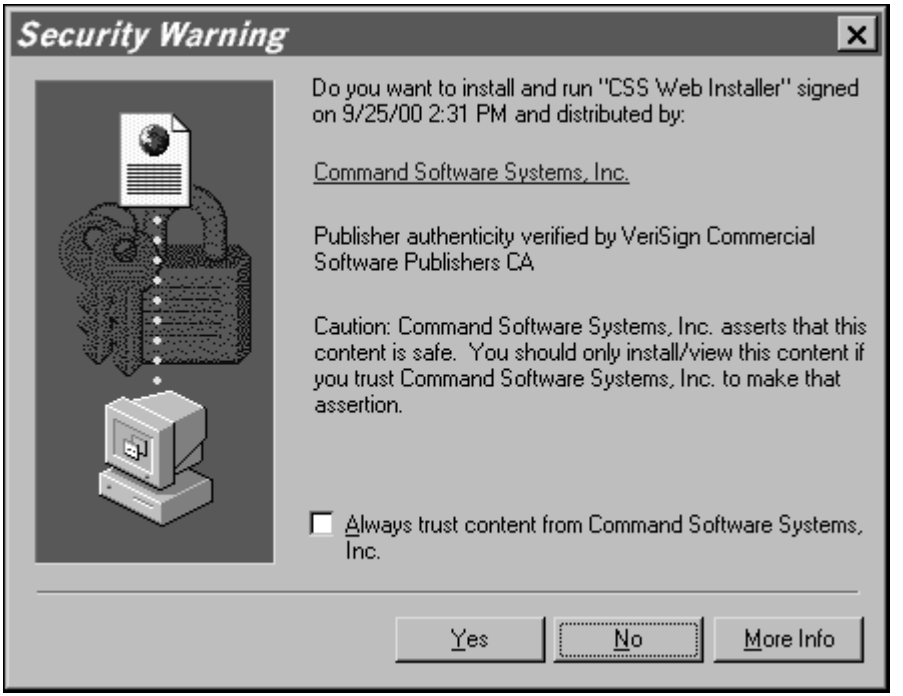
When you access Command On Demand, the program installs the plugins that work with your browser. The following section provides detailed instructions for Microsoft® Internet Explorer, Netscape® Communicator, and Netscape® 6 users.

**NOTE:** If you are using the **Biz Dev** version of Command On Demand, you **must** uninstall this version before you install the **Commercial** version. For information on uninstalling Command On Demand, refer to **Removing Command On Demand** located later in this chapter.

# INTERNET EXPLORER

**NOTE:** To install Command On Demand, ActiveX controls on your browser must be enabled.

Depending on which version of Internet Explorer you are using and the security levels that you have set, the system may display a **Security Warning** dialog box:




**Security Warning Dialog Box**

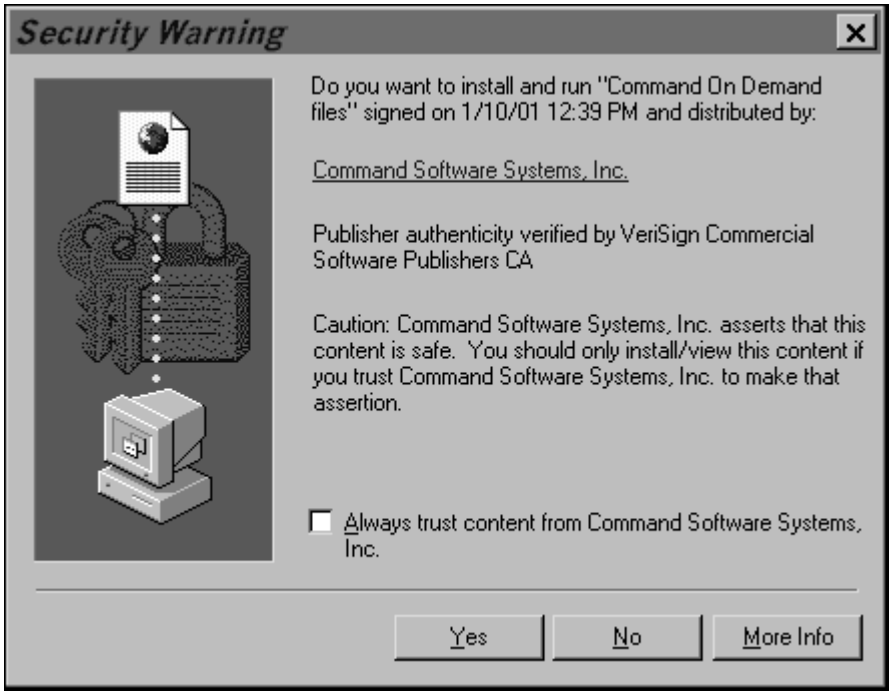
This dialog box asks if you want to install and run the CSS Web Installer.

We suggest that you select the **Always trust content from Command Software Systems, Inc.** check box. If you select this option, you will **not** be prompted again even when you access Command On Demand at a later time.

If you do **not** select this option, the system may display a **Security Warning** dialog box before installing the Command On Demand files.

To install the CSS Web Installer, click **Yes**. To stop the installation, select **No**.

**NOTE:** If you did **not** select the **Always trust content from Command Software Systems, Inc.** check box, the system may display the following **Security Warning** dialog box.




**Security Warning Dialog Box**

This dialog box asks if you want to install and run Command On Demand files.

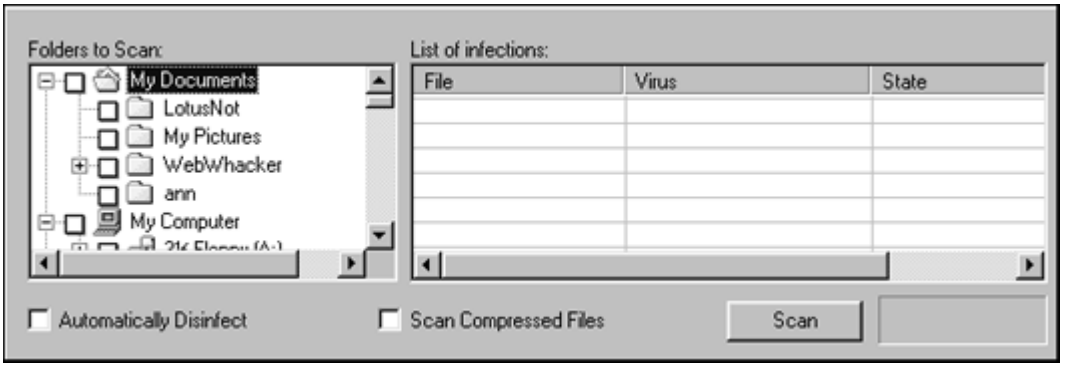
We suggest that you select the **Always trust content from Command Software Systems, Inc.** check box. If you select this option, you will **not** be prompted again when you access Command On Demand.

If you do **not** select this option, the system may display a **Security Warning** dialog box each time you access Command On Demand.

Click **Yes** to install the files.

**NOTE:** During the installation, the program downloads and installs the ATL Run-Time DLL. If you have an older version of this DLL installed, you may be asked to restart your computer after the new version of this component is installed. After your computer has restarted, restart your browser and reopen the Command On Demand page. The installation will continue automatically.

When the installation is complete, the system displays the **Command On Demand Main** dialog box:




**Command On Demand Main Dialog Box**

**NOTE:** If you are using the **Biz Dev** version of Command On Demand, the disinfection feature is **not** available.

# NETSCAPE

To use Command On Demand with your Netscape browser, you **must** first install the Asgard Installation Plugin and the CSS Web Installer for Netscape. The CSS Web Installer for Netscape allows you to download and install the Command On Demand files automatically. The Asgard Installation Plugin allows you to run the Command On Demand files in Netscape.

**NOTE:** If you already have the Asgard Installation Plugin installed on your computer, the program downloads only the CSS Web Installer and the Command On Demand files.

The Asgard Installation Plugin and the CSS Web Installer can be installed automatically or manually. The method of installation depends on the conditions that you have set:

- **If you have SmartUpdate enabled**, you can download and install the Asgard Installation Plugin, the CSS Web Installer, and the Command On Demand files automatically. For more information, refer to **Enabling SmartUpdate**.

**NOTE: Netscape 6 users** should enable Software Installation. For more information, refer to **Enabling Software Installation in Netscape 6**.

- **If you do not have SmartUpdate or Software Installation enabled**, you **must** install the Asgard Installation Plugin and the CSS Web Installer manually. When these plugins are installed, you can then install the Command On Demand files automatically.

**NOTE:** We strongly recommend that **only** experienced users install the Asgard Installation Plugin and the CSS Web Installer manually.

To install the plugins, depending on the conditions that you have set, follow the instructions in either **Automatic Installation** or **Manual Installation**.

**NOTE:** Netscape 6 users follow the instructions in either **Automatic Installation for Netscape 6 Users** or **Manual Installation for Netscape 6 Users**.

## Enabling SmartUpdate

**NOTE:** If you are using Netscape 6, go to **Enabling Software Installation in Netscape 6**.

To enable the SmartUpdate feature, follow these steps:

1. On the menu bar of your browser, click **Edit**.
2. From the drop-down menu, click **Preferences**.
3. In the **Preferences** tree, locate and click **Advanced**.
4. To the right, in the **Advanced** dialog box, select the **Enable Java** check box.
5. In the **Preferences** tree, click the plus sign **(+)** to the left of **Advanced** to expand the preferences.
6. From the expanded list, click **SmartUpdate**.
7. To the right, in the **SmartUpdate** dialog box, select the **Enable SmartUpdate** check box and click **OK**.
8. To start the installation, on the toolbar of your browser, click **Reload**.

## Enabling Software Installation in Netscape 6

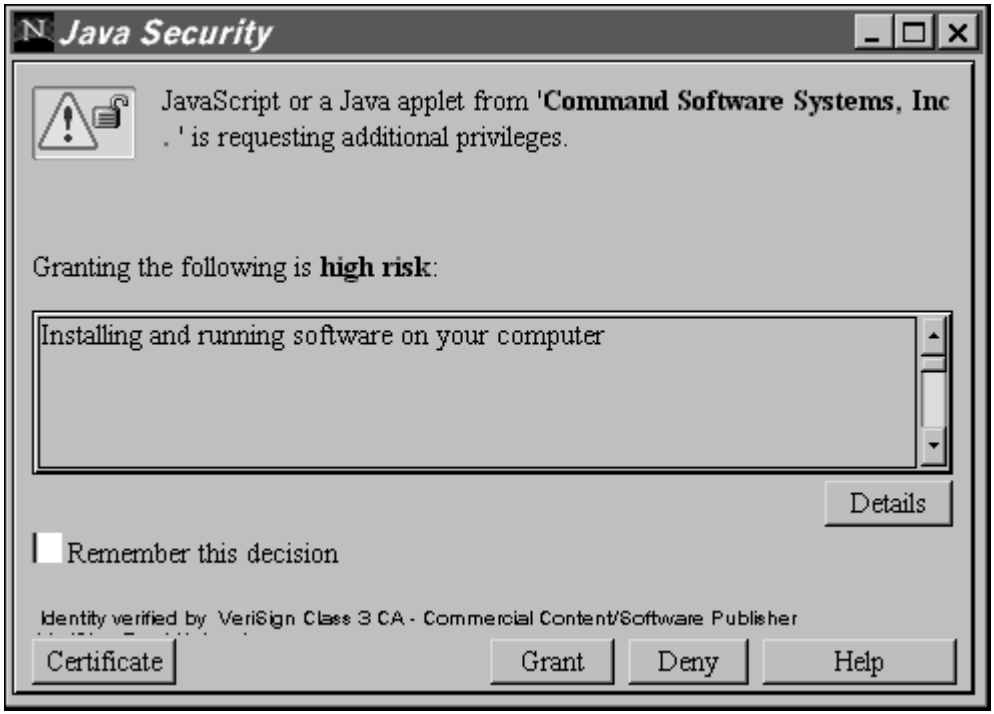
To enable the Software Installation feature in Netscape 6, follow these steps:

1. On the menu bar of your browser, click **Edit**.
2. From the drop-down menu, click **Preferences**.
3. In the **Preferences** tree, locate **Advanced**.
4. Click the forward arrow **(>)** to the left of **Advanced** to expand the preferences.
5. From the expanded list, click **Software Installation**.
6. To the right, in the **Software Installation** dialog box, select the **Enable software installation** check box and click **OK**.
7. To start the installation, on the menu bar of your browser, click **View**.
8. From the drop-down menu, click **Reload**.

## Automatic Installation

**NOTE:** If you are using Netscape 6, go to **Automatic Installation for Netscape 6 Users**.

If you have SmartUpdate enabled, you can download and install the Asgard Installation Plugin, the CSS Web Installer, and the Command On Demand files automatically. When you access the Command On Demand page, if you do not have the Asgard Installation Plugin or the CSS Web Installer installed, the system displays the following **Java Security** dialog box:




**Java Security Dialog Box**

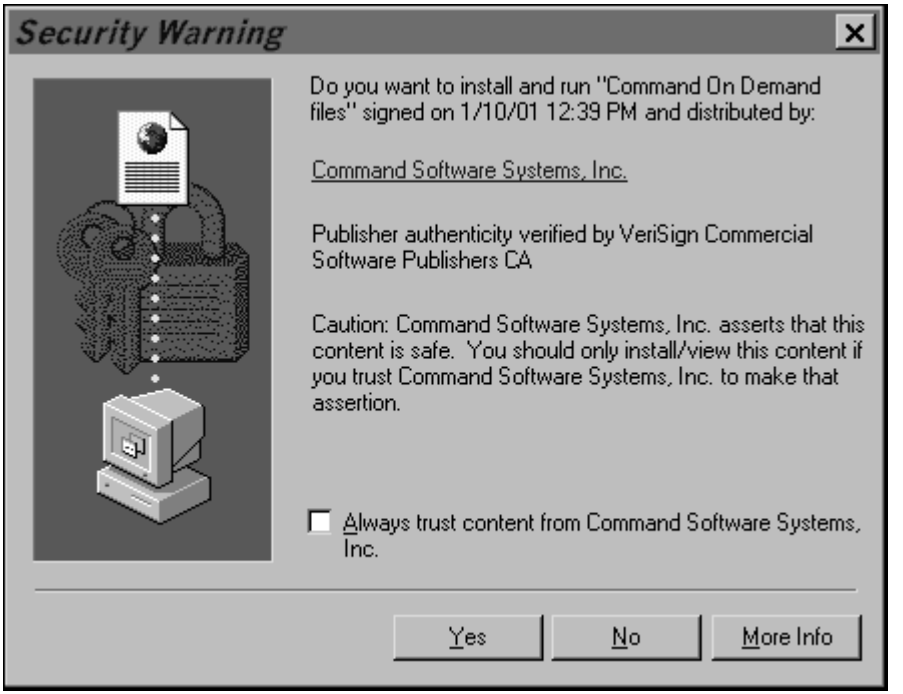
This dialog box asks if you want to install and run software from Command Software Systems, Inc.

We suggest that you select the **Remember this decision** check box. If you select this option, you will **not** be prompted again even if you update the Asgard Installation Plugin or the CSS Web Installer at a later time.

If you do **not** select this option, the system will display a **Security Warning** dialog box before installing any updates to the Asgard Installation Plugin and the CSS Web Installer.

Click **Grant** to begin the installation. When the installation is complete, the system displays the **Command On Demand Main** dialog box.

**NOTE:** Depending on the security levels that you have set, the system may display the following **Security Warning** dialog box.




**Security Warning Dialog Box**

This dialog box asks if you want to install and run Command On Demand files.

We suggest that you select the **Always trust content from Command Software Systems, Inc.** check box. If you select this option, you will **not** be prompted again when you access Command On Demand.

If you do **not** select this option, the system may display a **Security Warning** dialog box each time you access Command On Demand.

Click **Yes** to install the files. When the installation is complete, the system displays the **Command On Demand Main** dialog box.

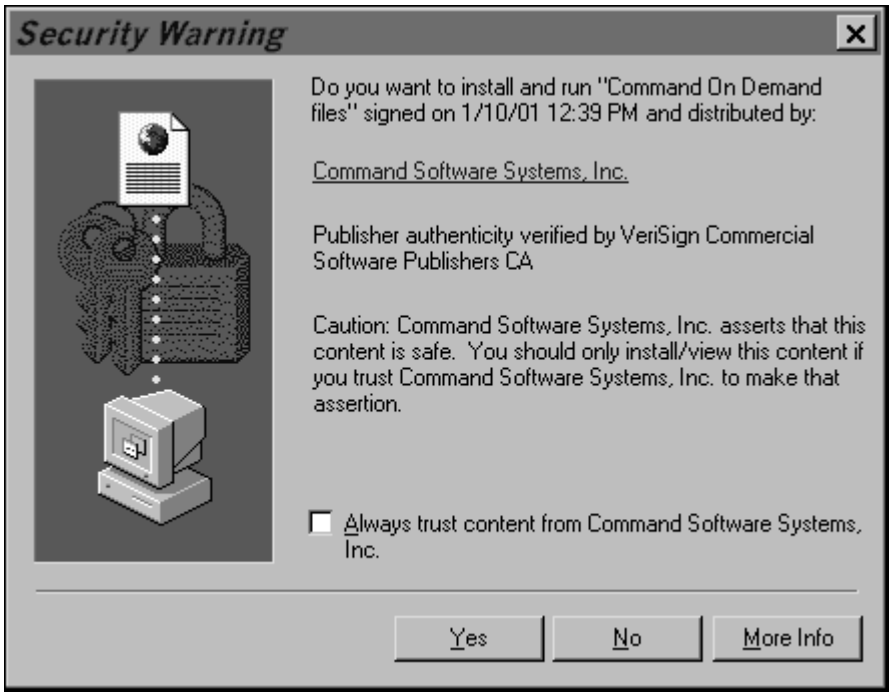
## Automatic Installation for Netscape 6 Users

If you have Software Installation enabled, you can download and install the Asgard Installation Plugin, the CSS Web Installer, and the Command On Demand files automatically. When you access the Command On Demand page, if you do not have the Asgard Installation Plugin and the CSS Web Installer installed, the system displays the following **Software Installation** security dialog box:

**Software Installation Security Dialog Box**

This dialog box asks if you want to install the software package. Click **OK**. When the system displays the **Please wait....** message, restart your browser and reopen the Command On Demand page. The installation continues automatically.

**NOTE:** Depending on the security levels that you have set, the system may display the following **Security Warning** dialog box.




**Security Warning Dialog Box**

This dialog box asks if you want to install and run Command On Demand files.

We suggest that you select the **Always trust content from Command Software Systems, Inc.** check box. If you select this option, you will **not** be prompted again when you access Command On Demand.

If you do **not** select this option, the system may display a **Security Warning** dialog box each time you access Command On Demand.

Click **Yes** to install the files.

When the system displays the Command On Demand banner, restart your browser and reopen the Command On Demand page. The installation continues automatically. When the installation is complete, the system displays the **Command On Demand Main** dialog box.

## Manual Installation

**NOTE:** If you are using Netscape 6, go to **Manual Installation for Netscape 6 Users**.

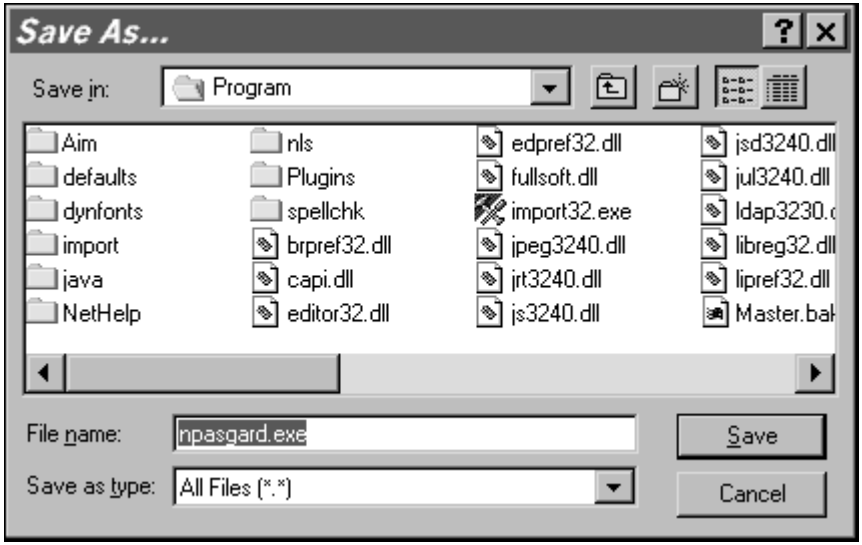
If you do not have SmartUpdate enabled, you **must** install the Asgard Installation Plugin and the CSS Web Installer manually. When you access the Command On Demand page, the system displays the **Asgard Installation Plugin and CSS Web Installer for Netscape** download page.

**NOTE:** If you already have an up-to-date version of the Asgard Installation Plugin installed on your computer, the system displays the **CSS Web Installer for Netscape** download page. This page allows you to download only the CSS Web Installer and the Command On Demand files.

This page allows you to download and install the Asgard Installation Plugin and the CSS Web Installer.

To download and install the Asgard Installation Plugin and the CSS Web Installer, follow these steps:

1. Click the link (**Click here**) to download the installer program and save it on your computer. The system displays the following dialog box:




**Save As Dialog Box**

2. Click **Save**.

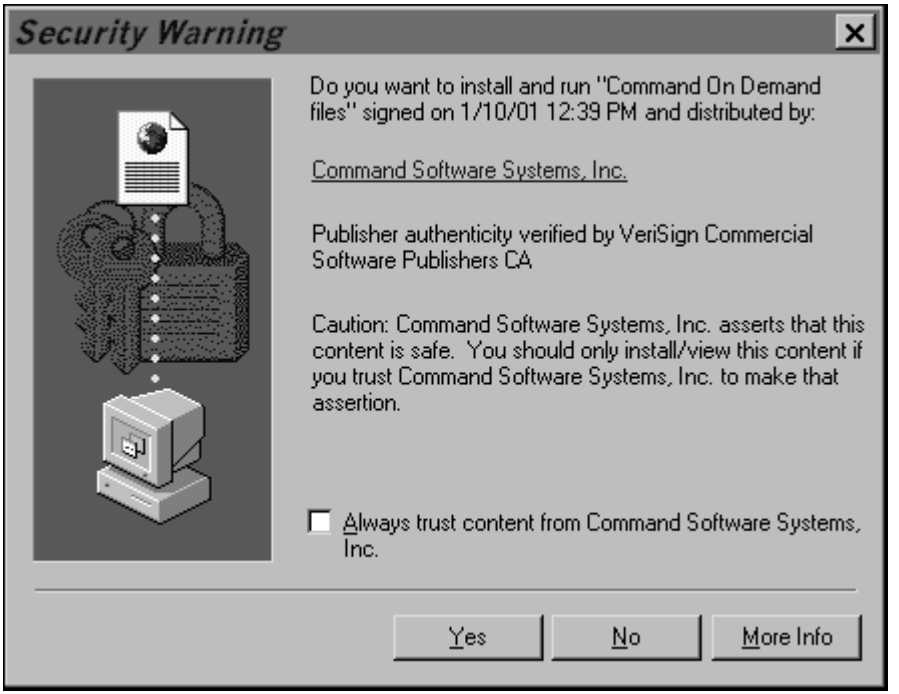
**NOTE:** Be sure to remember the path and file name of the installer program.

3. Run the installer program that you downloaded in **Step 1**.

**NOTE:** You do **not** need to close the browser session to run the installation.

When the installation of the Asgard Installation Plugin and the CSS Web Installer is complete, the Command On Demand installation begins automatically. When the Command On Demand installation is complete, the system displays the **Command On Demand Main** dialog box.

**NOTE:** Depending on the security levels that you have set, the system may display a **Security Warning** dialog box:




**Security Warning Dialog Box**

This dialog box asks if you want to install and run Command On Demand files.

We suggest that you select the **Always trust content from Command Software Systems, Inc.** check box. If you select this option, you will **not** be prompted again when you access Command On Demand.

If you do **not** select this option, the system may display a **Security Warning** dialog box each time you access Command On Demand.

Click **Yes** to install the files. When the files are installed, the system displays the **Command On Demand Main** dialog box.

## Manual Installation for Netscape 6 Users

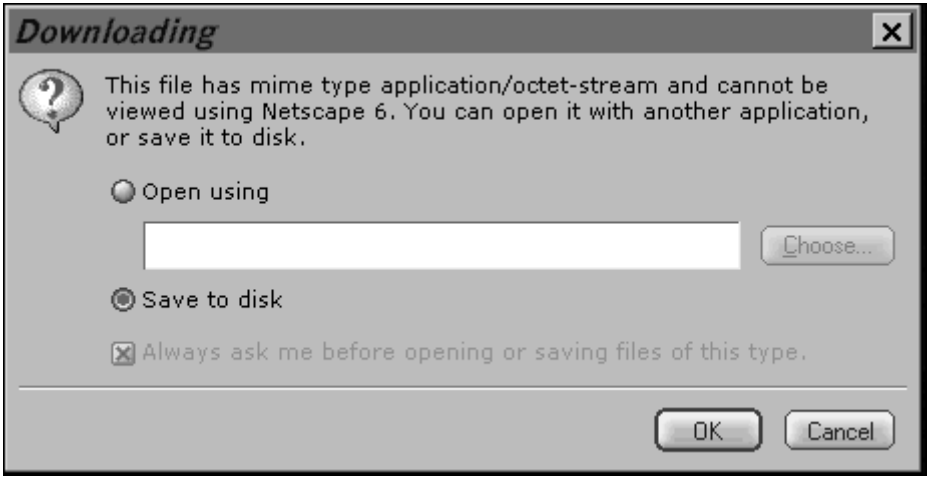
If you do not have Software Installation enabled, you **must** install the Asgard Installation Plugin and the CSS Web Installer manually. When you access the Command On Demand page, the system displays the **Asgard Installation Plugin and CSS Web Installer for Netscape** download page.

**NOTE:** If you already have an up-to-date version of the Asgard Installation Plugin installed on your computer, the system displays the **CSS Web Installer for Netscape 6** download page. This page allows you to download only the CSS Web Installer and the Command On Demand files.

This page allows you to download and install the Asgard Installation Plugin and the CSS Web Installer.

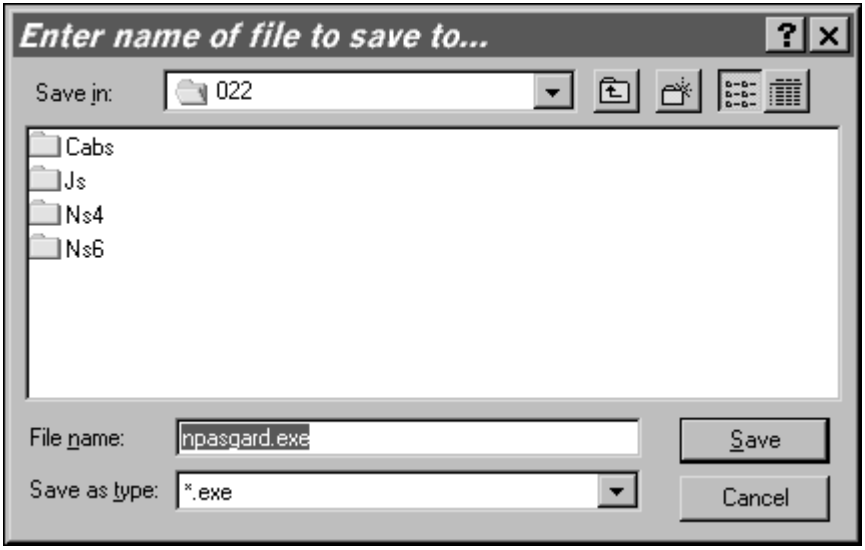
To download and install the Asgard Installation Plugin and the CSS Web Installer, follow these steps:

1. Click the link (**Click here**) to download the installer program and save it to a **temporary** folder on your computer. The system displays the following dialog box:




**Downloading Dialog Box**

2. Select **Save to disk**, and click **OK**. The system displays the **Enter name of file to save to....** dialog box:



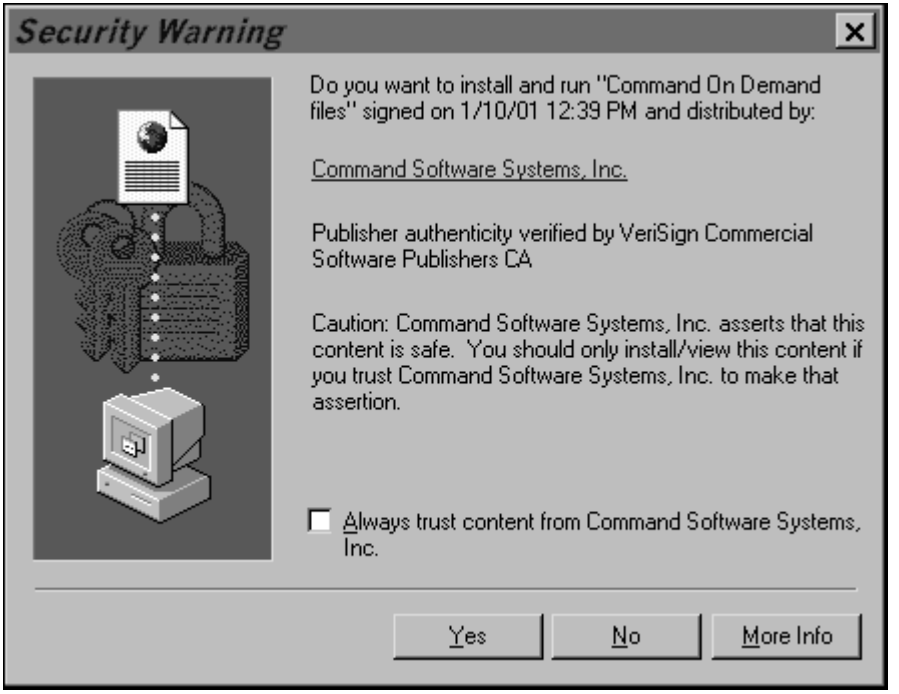

**Save to Dialog Box**

3. In the **Save in** drop-down box, select a temporary folder, and click **Save**.

**NOTE:** Be sure to remember the path and file name of the installer program.

4. Run the installer program that you downloaded in **Step 1**.
5. When the installation of the Asgard Installation Plugin and the CSS Web Installer is complete, restart your browser and reopen the Command On Demand page. The installation continues automatically.

**NOTE:** Depending on the security levels that you have set, the system may display a **Security Warning** dialog box:




**Security Warning Dialog Box**

This dialog box asks if you want to install and run Command On Demand files.

We suggest that you select the **Always trust content from Command Software Systems, Inc.** check box. If you select this option, you will **not** be prompted again when you access Command On Demand.

If you do **not** select this option, the system may display a **Security Warning** dialog box each time you access Command On Demand.

Click **Yes** to install the files.

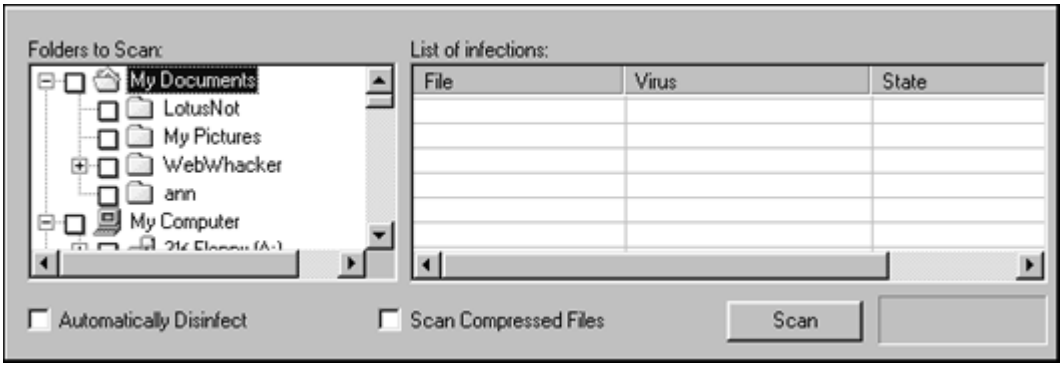
When the system displays the Command On Demand banner, restart your browser and reopen the Command On Demand page. The installation continues automatically.

When the installation is complete, the system displays the **Command On Demand Main** dialog box.

# THE COMMAND ON DEMAND MAIN DIALOG BOX

Command On Demand uses a Graphical User Interface (GUI) that allows you to start a virus scan quickly and easily. The main screen of the GUI is called the **Command On Demand Main** dialog box:






**Command On Demand Main Dialog Box**

From the **Command On Demand Main** dialog box, you can perform several scan task operations. For example, you can select the drives and folders that you want to scan, include compressed files to be scanned, start or stop a virus scan, and disinfect an infected file.

**NOTE:** If you are using the **Biz Dev** version of Command On Demand, the disinfection feature is **not** available.

# COMPONENTS

The **Command On Demand Main** dialog box is simple and easy to use. The following information will help you become familiar with its components:

## Folders to Scan

The **Folders to Scan** list allows you to select the drives and folders that you want to scan. To select a drive or folder, click the check box to the left of the drive or folder name. The system places a check mark in the box to indicate that the driver or folder is selected. To clear the check box, click it again.

**NOTE:** When you select a subfolder, a dimmed check mark is placed in the check box to the left of the drive and the root folder as a place marker. The entire drive and the root folder are **not** scanned.

You cannot select only the root folder of a subdirectory branch. If you select the root folder all subfolders are selected automatically. To remove certain subfolders from the scan, clear the check box to the left of each folder.

**NOTE:** When a scan is complete, the drives and folders remain selected until you clear the check boxes or exit the program.

## List of Infections

When the scan is complete, the **List of infections** displays information about the infected files. For example, you can view the name of the infected file, the name of the virus, and the present state of the file – whether it is infected or disinfected. You can also view the path of the infected file, by placing the mouse pointer on the file name.

## Automatically Disinfect

The **Automatically Disinfect** check box allows you to disinfect infected files automatically as they are detected during the scan.

**NOTE:** If you are using a **Biz Dev** version of Command On Demand, the disinfection feature is **not** available.

## Scan Compressed Files

Command On Demand scans compressed files, but does **not** disinfect them.

The **Scan Compressed Files** check box allows you to include compressed files in the scan. Compressed files include:

- **Packed files** – Executable programs that have been compressed with ICE-packed, DIET, LZEXE-packed, PKLITE, and WWPack.
- **Non-executable compressed files** – Non-executable files that have been archived using programs such as PKWare's ZIP and ARJ compression utilities.
- **Executable compressed files** – Executable files that have been archived using programs such as PKWare's ZIP compression utility.

## Scan

The **Scan** button allows you to start an on-demand scan. Select the drives or folders that you want to scan and click **Scan**.

## Stop Scan

When a scan is in progress, the **Scan** button changes to the **Stop Scan** button. The **Stop Scan** button allows you to quit a scan.

## Activity Indicator

The activity indicator is located to the right of the **Stop Scan** button. The activity indicator displays the names of the files as they are being scanned.

# USING COMMAND ON DEMAND MAIN DIALOG BOX

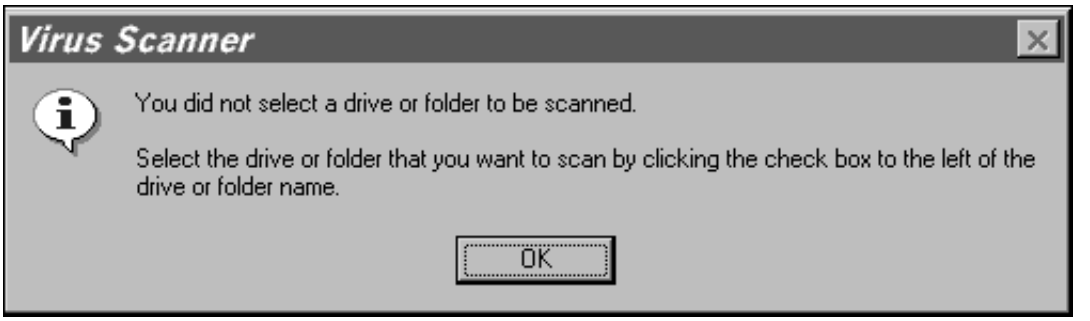
This section provides instructions on how to start a scan and how to disinfect files.

## STARTING A SCAN

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

1. From the **Folders to Scan** list, select a drive or folder to scan by selecting the check box to the left of the drive or folder name.

**NOTE:** If you do not make a selection, the system displays an error dialog box:




**Error Dialog Box**

Click **OK** to exit this dialog box and make your selections.

**NOTE:** Command On Demand does **not** scan compressed files by default. If you want to include compressed files in the scan, select the **Scan Compressed Files** check box.

The default setting for the action to take when a virus is found is report only. If you want to disinfect infected files when they are found, select the **Automatically Disinfect** check box.

**NOTE:** If you are using the **Biz Dev** version of Command On Demand, the disinfection feature is **not** available.

2. Click **Scan**. The scan begins. When the scan is complete, the system displays a results dialog box that contains details of the scan.

   These details include the:

   - number of files scanned
   - number of files infected
   - number of viruses detected
   - number of viruses disinfected

3. Click **OK** to close the dialog box.

If necessary, you can perform an on-demand scan that is set to **Automatically Disinfect**.

**NOTE:** If you are using the **Biz Dev** version of Command On Demand, the disinfection feature is **not** available.

## STOPPING A SCAN

To Stop a scan, follow these steps:

1. Click **Stop Scan**. The system displays a confirmation dialog box asking you to confirm that you want to cancel the scan.
2. Click **OK**. When the scan stops, the system displays a results dialog box that contains details of the scan.
3. Click **OK** to exit.

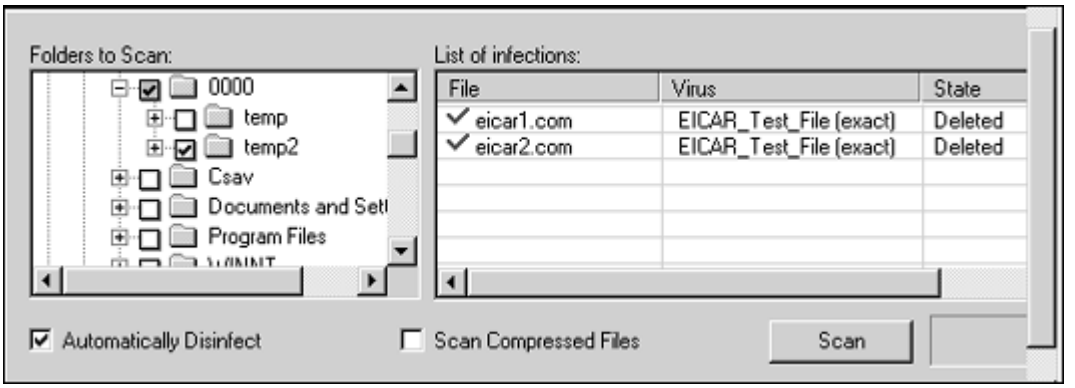
# DISINFECTING INFECTED FILES

**NOTE:** If you are using the **Biz Dev** version of Command On Demand, the disinfection feature is **not** available.

There are two ways to disinfect virus infected files. They are:

- Disinfecting automatically during the scan by selecting the **Automatically Disinfect** check box.
- Disinfecting manually during or after the scan by selecting a file or files in the **List of infections**. Then, using the right mouse button (right-clicking), click your selection(s). The system displays a drop-down menu. Click **Disinfect**.

When Command On Demand disinfects a file, in the **List of infections**, a red check mark displays to the left of the infected file name and the **State** is specified as **Disinfected**. If the only way to eliminate the virus is to delete the file, the **State** is specified as **Deleted.**




**Command On Demand Main Dialog Box – List of Infections View**

# ON-ACCESS PROTECTION

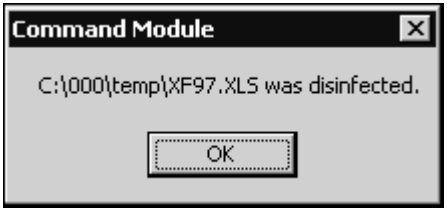
**NOTE:** The **On-access Protection** section applies only to the Virus Striker version of Command On Demand.

The Command Module for Office (CMO) plugin, provides on-access scanning for Microsoft Office 2000 and Microsoft Internet Explorer 5.x or higher.

## DOCUMENTATION FILES

Each time you open files in Microsoft Word, Power Point, and Excel, the Command Module for Office automatically scans the files for viruses. If a virus is found, CMO then attempts to disinfect the infected file. When the action is complete, the system displays a status dialog box.

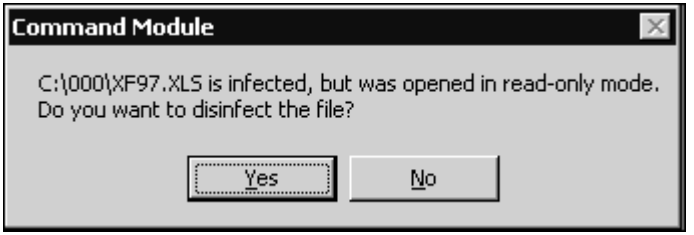
For example, if you open an infected Excel file, and CMO successfully disinfects the file, the system displays a **Disinfect Status Dialog Box**:




**Disinfect Status Dialog Box**

Click **OK** to exit.

**NOTE:** If the file that you open is **Read-only**, you may first receive a **Notification Dialog Box**:




**Notification Dialog Box**

This dialog box informs you that the infected file is read-only. It then asks you if you want to disinfect the file.

Click **YES** to disinfect the file. Click **NO** to exit.

If you click **YES,** CMO attempts to disinfect the infected file. If the file cannot be disinfected, CMO attempts to rename the file with an **.INFECTED** extension. When the action is complete, the system displays a status dialog box.

In some instances, for example a shared file, Command Module for Office is **not** able to disinfect or rename the file. The system then displays a **Failure to Disinfect Status Dialog Box**:

**Failure to Disinfect Status Dialog Box**

This file is still infected. As a result of certain programming limitations, when you click **OK** to exit the **Failure to Disinfect Status Dialog Box**, the Microsoft Office application opens the infected file.

We recommend that you run a manual scan of your hard drive using Command On Demand to disinfect this file and any other files that might be infected.

## DOWNLOADING

Command Module for Office also automatically scans and disinfects files that are downloaded and installed through Internet Component Download (ICD) in Microsoft Internet Explorer Version 5.x or higher.

For example, if you download and install an infected **.EXE** file through ICD, CMO attempts to disinfect **only** a copy of the file that was downloaded to your computer. If the disinfection is successful, the system displays a **Disinfect Download Status Dialog Box**:

**Disinfect Download Status Dialog Box**

**NOTE:** You should notify the owner of the document that the file is infected.

**NOTE:** Command Module for Office does **not** disinfect compressed files, for example, **.CAB** files. To disinfect compressed files, uncompress the file and run an on-demand scan using Command On Demand. Then, recompress the file.

Click **OK** to exit.

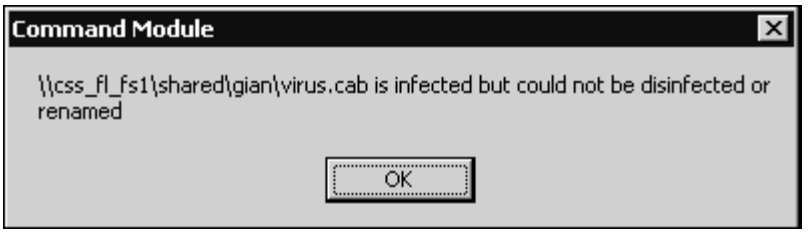
**NOTE:** If the file that you open is **Read-only**, you may first receive a **Notification Dialog Box.**

This dialog box informs you that the infected file is read-only. It then asks you if you want to disinfect the file.

Click **YES** to disinfect the file. Click **NO** to exit.

If you click **YES,** CMO attempts to disinfect the infected file. If the file cannot be disinfected, CMO attempts to rename the file with an **.INFECTED** extension. When the action is complete, the system displays a status dialog box.

In some instances, for example a shared file, Command Module for Office is **not** able to disinfect or rename the file. The system then displays a **Failure to Disinfect Status Dialog Box**:




**Failure to Disinfect Status Dialog Box**

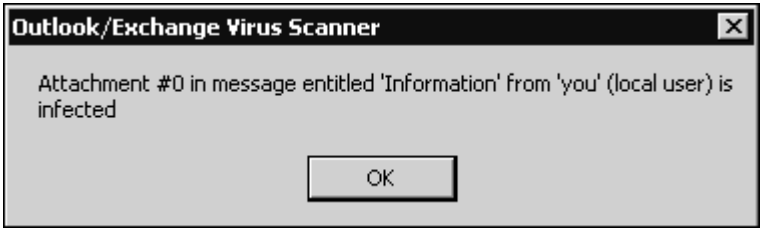
This file is still infected. As a result of certain programming limitations, when you click **OK** to exit the **Failure to Disinfect Status Dialog Box**, the Microsoft Office application opens the infected file.

We **strongly** recommend that you close the application and use Command On Demand to perform a scan of your hard drive. If Command On Demand cannot disinfect or delete the infected file, contact your technical support provider for this program or delete the file.

Click **OK** to exit.

# E-MAIL MESSAGES

If you are logged into Microsoft Exchange client or Microsoft Outlook, Command Module for Office is also at work when you send or receive infected e-mail messages. As soon as you receive an e-mail into your mailbox or click **Send** to send an e-mail, CMO scans the body and the attachments of the e-mail. This scan includes shortcuts to infected files, embedded files in the message, and embedded messages. If a virus is found, CMO displays a **Mail Notification Dialog Box**:




**Mail Notification Dialog Box**

This dialog box informs you of the:

- Attachment Number
- E-mail Subject
- Sender's Name

Click **OK** to exit. CMO then attempts to disinfect the attachment. If the disinfection is successful, the program displays the **Disinfect Attachment Status Dialog Box:**

**Disinfect Attachment Status Dialog Box**

Click **OK** to exit.

If Command Module for Office is **not** able to disinfect a file, it deletes the file. The system then displays the **Failure to Disinfect Attachment Status Dialog Box**:

**Failure to Disinfect Attachment Status Dialog Box**

Click **OK** to exit.

# TROUBLESHOOTING

The following section provides information on what to do if Command On Demand fails to install properly. It also contains information on what to do if you try to install an incompatible version of Command On Demand.

For additional troubleshooting information, visit our web site at:

http://www.commandsoftware.com/service/index.html

## FAILURE TO INSTALL

If Command On Demand fails to install, you must remove all of the Command On Demand files before you try to reinstall.

After you remove all of the Command On Demand files, double-click the Command On Demand icon on your desktop to continue with the installation.

**NOTE:** As the Command On Demand icon may not have been installed, we recommend that you copy the URL of the page that you are installing from so that you can easily return to the installation page.

To remove the Command On Demand files, follow these steps:

**If you are using Microsoft Internet Explorer:**

1. On the Windows installation drive, locate the **CSSCOD** folder.
2. Delete this folder.

**NOTE:** If you cannot delete this folder, some of the files may be in use. Close all all Microsoft Office 2000 programs and all sessions of Microsoft Internet Explorer. Then, delete the folder.

3. Open Internet Explorer.
4. On the menu bar, click **View** or **Tools**. The system displays a drop-down menu.
5. Click **Internet Options**. The system displays the **Internet Options** dialog box.

6. Under **Temporary Internet files**, click the **Settings** button. The system displays the **Settings** dialog box.
7. Under **Temporary Internet files folder**, click the **View Objects** button. The system displays the **Download Program Files** page.
8. In the **Program File** window, locate the **CSS Web Installer Class**.
9. Using the right mouse button (right-click), click the file. The system displays a drop-down menu.
10. Click **Remove** to delete the file.

**If you are using Netscape Communicator:**

1. On the Windows installation drive, locate the **CSSCOD** folder.
2. Delete this folder.

**NOTE:** If you cannot delete this folder, some of the files may be in use. Close all sessions of your browser that contain the Command On Demand graphical user interface (GUI) and all Microsoft Office 2000 programs. Then, delete the folder.

3. On the Windows installation drive, locate the **Program Files** folder, and click the plus sign (**+**) to the right of the folder.
4. Locate the **Netscape** folder, and click the plus sign (**+**) to the right of the folder.
5. Locate the **Communicator** folder, and click the plus sign (**+**) to the right of the folder.
6. Locate the **Program** folder, and click the plus sign (**+**) to the right of the folder.
7. Locate and double-click the **Plugins** folder.
8. Locate and delete the following files:

   - NPCSSWEB.DLL
   - NPCODCS.DLL
   - NPCODCS.CLASS

**NOTE:** To delete a file, using the right mouse button (right-click), click the file. The system displays a drop-down menu. Click **Remove**.

**If you are using Netscape 6:**

The path to the files is **Program Files/Netscape/Netscape 6/Plugins**.

## INCOMPATIBLE VERSION

If you try to install an incompatible version of Command On Demand, you must uninstall the original version, and then install the new version. For more information on removing Command On Demand, refer to **Removing Command On Demand** located later in this chapter.

After you uninstall, double-click the Command On Demand icon on your desktop to continue with the installation of the new version.

**NOTE:** As the Command On Demand icon may not have been installed, we recommend that you copy the URL of the page that you are installing from so that you can easily return to the installation page.



# REMOVING COMMAND ON DEMAND

**NOTE: If you are using Microsoft Internet Explorer:** Be sure to close all Microsoft Office 2000 programs and all sessions of Microsoft Internet Explorer. If you do not, some of the files may be in use, and you will need to restart your computer after you uninstall.

**If you are using Netscape Communicator:** Be sure to close all sessions of your browser that contain the Command On Demand graphical user interface (GUI) and all Microsoft Office 2000 programs. If you do not, some of the files may be in use, and you will need to restart your computer after you uninstall.

To remove Command On Demand, follow these steps:

1. On the Windows taskbar, click the **Start** button.
2. Select **Settings**.
3. Click **Control Panel**.
4. Double-click the **Add/Remove Programs**. The system displays the **Add/ Remove Programs** dialog box.
5. Select **Command On Demand** from the list of currently installed programs.
6. Click the **Add/Remove** or **Remove** button. The system displays a confirmation dialog box asking you if you want to completely remove Command On Demand and its components.
7. Click **Yes**. The system displays a confirmation dialog box letting you know that Command On Demand has been removed.

**NOTE:** If you are using Internet Explorer, the system displays an **Error** dialog box. Just click **OK** to close the dialog box.

8. Click **OK**. The system returns to the **Add/Remove Programs** dialog box.
9. Click **OK** to exit.

# GLOSSARY

## BOOT SECTOR

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

## BOOT SECTOR VIRUS

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

## CIRCULAR INFECTION

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

## CMOS

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

## COMPANION VIRUS

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

## CROSS-LINKED FILES

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

## DROPPER

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

## EICAR TEST FILE

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

## ENCRYPTION

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

## EXECUTABLE CODE

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

## FALSE POSITIVE

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

## FILE STEALTH

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

## FULL STEALTH

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

## HEURISTICS

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

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

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

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

## INTEGRITY CHECKER

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

## JOKE PROGRAMS

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

## LOGIC BOMB

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

## MALWARE

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

## MACRO VIRUS

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

## MASTER BOOT RECORD (MBR)

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

## MEMORY-RESIDENT

Residing in computer memory as opposed to on the disk.

## MULTIPARTITE

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

## ON-ACCESS SCAN

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

## ON-DEMAND SCAN

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

## PARTITION TABLE

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

## POLYMORPHISM

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

## SCHEDULED SCAN

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

## STEALTH VIRUS

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

## TROJAN (OR TROJAN HORSE)

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

## TUNNELING

A characteristic of some viruses that try to access the operating system directly, bypassing any TSRs (including anti-virus software) that have been loaded.

## VIRUS

An independent program that reproduces itself. A virus may attach to other programs; it must create copies of itself (see the glossary entry for **Companion Viruses***).* It may attach itself to any executable code, including but not limited to boot sectors and/or partition sectors of hard and/or floppy disks. It may damage, corrupt or destroy data, or degrade system performance.

## VIRUS SIMULATOR

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

## VIRUS VARIANT

A modification of a previously known virus, a variation.

## WORM

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