

**Command AntiVirus™**  
**for**  
**Unix®**

**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 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. CU-474-1002

Part No. 07-1000-00

# 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 - CSAV for Linux .....	1-2
Chapter 3 - CSAV for Solaris .....	1-2
Chapter 4 - CSAV for FreeBSD .....	1-2
Conventions Used .....	1-3
Additional Information .....	1-4
Web Site .....	1-4
Mailing List Server .....	1-4
README.TXT .....	1-4
<b>CSAV FOR LINUX .....</b>	<b>2-1</b>
Pre-installation Requirements .....	2-1
Installing .....	2-1
Verifying the Installation .....	2-5
Location of Installed Files .....	2-6
Testing Command AntiVirus .....	2-8
Updating Command AntiVirus for Linux .....	2-8
Updating the Definition Files .....	2-9
Scheduling Updates .....	2-10
Performing a Virus Scan .....	2-11
Command-line Options .....	2-11
Removing Command AntiVirus .....	2-16
<b>CSAV FOR SOLARIS .....</b>	<b>3-1</b>
Pre-installation Requirements .....	3-1
SPARC Platform .....	3-1
Intel Platform .....	3-1
Installation .....	3-2
Installing Using the Pkgadd Command .....	3-3
Installing Using Admintool .....	3-6
Location of Installed Files .....	3-17
Testing Command AntiVirus .....	3-20
Updating the Definition Files .....	3-20
Performing a Virus Scan .....	3-21
Command-line Options .....	3-22
Removing Command AntiVirus .....	3-27
From the Command Prompt .....	3-27
Using Admintool .....	3-28

---

<b>CSAV FOR FREEBSD .....</b>	<b>4-1</b>
Pre-installation Requirements .....	4-1
Installing .....	4-1
Verifying the Installation .....	4-4
Location of Installed Files .....	4-5
Testing Command AntiVirus .....	4-7
Updating Command AntiVirus for FreeBSD .....	4-7
Updating the Definition Files .....	4-8
Scheduling Updates .....	4-9
Performing a Virus Scan .....	4-9
Command-line Options .....	4-10
Removing Command AntiVirus .....	4-15



# INTRODUCTION

Command AntiVirus (CSAV) for Unix® is a command-line scanner. Command Software Systems provides different packages for the Linux®, the Solaris™, and the FreeBSD operating systems. Command AntiVirus provides state-of-the-art antivirus protection through HoloCheck™ scanning technology. The most important benefits of this technology are:

- Simplified antivirus updates. You can now update the **sign.def**, **sign2.def**, and **macro.def** files (which contain the latest virus signatures) without reinstalling all of CSAV's components. This updating method adds speed and efficiency to Command AntiVirus.
- Superior polymorphic virus detection. Command AntiVirus now offers unparalleled protection and elimination of polymorphic viruses including the dreaded Morphine, Anxiety, Spanska, Magistr and MTX.
- Scanning of embedded (OLE) documents. Not only do we scan documents, but if an infected document is embedded in an Excel spreadsheet or a PowerPoint document, Command AntiVirus will detect it and prevent your data from becoming infected.

## MAIN FEATURES

---

Command AntiVirus is a comprehensive virus protection program that:

- Uses state-of-the-art technology to scan for tens of thousands of known viruses and their variants.
  - Removes viruses without damaging the original file.
  - Scans for images of boot sector viruses, macro viruses, and Trojan Horses.
-

- Scans hard drives, diskettes, CD-ROMs, network drives, directories, and specific files.
- Scans archived files, compressed files, and compressed executables.
- Can be configured to perform scheduled scans when used with the Unix **cron** utility.

## CHAPTER OVERVIEW

---

The *Command AntiVirus for Unix User's Guide* consists of the following chapters.

### CHAPTER 1 - INTRODUCTION

This chapter provides an overview of Command AntiVirus including a list of features and conventions.

### CHAPTER 2 - CSAV FOR LINUX

Chapter 2 provides pre-installation requirements and instructions on installing and removing Command AntiVirus for Linux. This chapter also includes information on performing virus scans, using the product's command line switches, and using the Command AntiVirus for Linux e-mail notification feature.

### CHAPTER 3 - CSAV FOR SOLARIS

This chapter provides pre-installation requirements and instructions on installing and removing Command AntiVirus for Solaris™ on both the SPARC® and Intel® platforms. Chapter 3 also includes information on performing virus scans, using the product's command-line switches, and using the Command AntiVirus for Solaris e-mail notification feature.

### CHAPTER 4 - CSAV FOR FREEBSD

This chapter provides pre-installation requirements and instructions on installing and removing Command AntiVirus for FreeBSD. Chapter 4 also includes information on performing virus scans, using the product's command-line switches, and using the Command AntiVirus for FreeBSD e-mail notification feature.

## 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:

```
CSAV -HARD -DISINF
```

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

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

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

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

---

## 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, visit our web site.

### README.TXT

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



# CSAV FOR LINUX



## PRE-INSTALLATION REQUIREMENTS

---

The system requirements for Command AntiVirus for Linux® are:

- An IBM®-compatible computer with a 386 or higher CPU
- Red Hat® Linux Version 6.0 or higher, or SuSE® Linux 6.2 or higher
- At least 4.0 MB of available hard disk space
- GLIBC\_2.0 or GLIBC\_2.1 “C” runtime library



**NOTE:** Command AntiVirus for Linux may work on any Linux that uses GLIBC 2.0 or higher and kernel 2.0 or higher.

## INSTALLING

---

Installing Command AntiVirus for Linux is easy to do. The installation places all of the required CSAV files in the necessary directories.

Before beginning, please read the installation instructions thoroughly. This will help you to anticipate any choices that you may need to make during the installation process.

Command AntiVirus for Linux consists of three packages: Command AntiVirus scan engine, the virus definition files also referred to as deffiles, and the documentation.

---

The documentation package installs the translated versions of the following:

- **readme.txt** – contains important last-minute information about the functioning of the product.
- **guide.txt** – the short form of the *Command AntiVirus for Unix User's Guide* in text format.
- **distrib.txt** – contains contact information about all of the Command Software distributors.
- **legal.txt** – contains legal information on product copyright, licensing, usage, etc.
- **email.cfg** – a sample e-mail notification file. This file can be used when **-notify=user@domain** is provided.



**NOTE:** Administrators can use a text editor to change the content of **email.cfg** to fit their needs.

- **cssunix.pdf** – the *Command AntiVirus for Unix User's Guide*.



**NOTE:** The English versions of the first five files are installed when you install the Command AntiVirus package. The **cssunix.pdf** file is **not** installed unless you install the documentation package.

To install Command AntiVirus for Linux, follow these steps:

1. At the Linux command prompt, **\$**, type the following and press **Enter** to determine whether your system is using **glibc2**:

```
ldd /bin/ls | grep libc | awk '{print $1; }'
```

If the output from this command is the following, you are using GLIBC as the primary library and should continue with Step 2:

```
libc.so.6
```

If you are not using GLIBC you must install it before continuing with the installation.

2. At the Linux command prompt, **\$**, type the following, and press **Enter**:

```
su
```

The system displays the **Password:** prompt.

3. Type your root password and press **Enter**.
4. At the command prompt, **#**, type the following, and press **Enter**:

```
mount /mnt/cdrom
```

5. To install the Command AntiVirus package, at the command prompt, type the following, and press **Enter**:

```
rpm -i /mnt/cdrom/CSAV/linux/csav-x.xx.x-shared.i386.rpm
```

The **x.xx.x** represents the Command AntiVirus version number, for example, 4.70.0.

6. To install the deffiles package, at the command prompt, type the following, and press **Enter**:

```
rpm -i /mnt/cdrom/CSAV/linux/csav/linux/deffiles-yyyymmdd-shared.noarch.rpm
```

The **yyyy** represents the year the deffiles were released. The **mm** represents the month, and the **dd** represents the day, for example, **20010912**. As a result, the deffiles package name changes when an updated package is released.

7. To install the documentation package, at the command prompt, type the following, and press **Enter**:

```
rpm -i /mnt/cdrom/CSAV/linux/csav-docs-x.xx.x-language.rpm
```

The **x.xx.x** represents the Command AntiVirus version number, for example, 4.70.0. The **language** represents the language used, for example, **english**.

8. To complete the installation of Command AntiVirus for Linux, at the command prompt, type the following, and press **Enter**:

```
exit
```

The system returns to the Linux command prompt, **\$**.

## VERIFYING THE INSTALLATION

To verify that the Command AntiVirus package is installed properly, at the command prompt, \$, type the following and press **Enter**:

```
rpm -q csav
```

The system displays the following message:

```
csav-x.xx.x-shared
```

The **x.xx.x** represents the Command AntiVirus version number, for example, 4.62.2. This version number confirms the installation.

To verify that the deffiles package is installed properly, at the command prompt, \$, type the following and press **Enter**:

```
rpm -q deffiles
```

The system displays the following message:

```
deffiles-yyyyymmdd-shared
```

The **yyyy** represents the year the deffiles were released. The **mm** represents the month, and the **dd** represents the day, for example, **20010912**.

To verify that the documentation package is installed properly, at the command prompt, \$, type the following and press **Enter**:

```
rpm -q csav-docs
```

The system displays the following message:

```
csav-docs-x.xx.x-language
```

The **x.xx.x** represents the Command AntiVirus version number, for example, 4.70.0. The **language** represents the language used, for example, **english**.

## LOCATION OF INSTALLED FILES

For updating or troubleshooting purposes, you may need to know the location of the Command AntiVirus files that were installed on your system. For example, when you update the **macro.def**, **sign2.def**, and **sign.def** files, you may need to know their locations. **Table 1** and **Table 2** provide the locations for the shared and static package files.

**Table 1: Installed Locations of CSAV for Linux Files – CSAV Package**

Path	Description
/usr/bin/csav	The Command AntiVirus command-line scanner.
/usr/lib/libcscan.so	A symbolic link to the most recently installed shared library.
/usr/lib/libcscan.so.x.xx	The shared library for CSAV. The <b>x.xx.x</b> represents the version number of the product, for example, <b>4.70.0</b> . <b>Note:</b> The <b>/usr/lib/libcscan.so</b> path mentioned above links to this specific file.
/etc/csav/english.tx1	The file containing language-specific text.
/etc/csav/email.cfg	A sample e-mail notification file. This file can be used when <b>-notify=user@domain</b> is provided. <b>Note:</b> Administrators can use a text editor to change the content of <b>email.cfg</b> to fit their needs.
/usr/doc/csav/distrib.txt	This file provides contact information about all of the Command AntiVirus distributors.
/usr/doc/csav/readme.txt	The readme file for Command AntiVirus for Linux. This file contains important last-minute information about the functioning of the product.
/usr/doc/csav/legal.txt	This file contains legal information on product copyright, licensing, usage, etc.
/usr/doc/csav/guide.txt	The <i>Command AntiVirus for Unix User's Guide</i> short form in text format.
/usr/man/man1/csav.1.gz	The online manual page.

**Table 2: Installed Locations of CSAV for Linux Definition Files – Deffiles Package**

Path	Description
/etc/csav/macro.def	The virus signature definition file for macro viruses.
/etc/csav/sign.def	The virus signature definition file for non-macro viruses.
/etc/csav/sign2.def	The virus signature extended definition file.

**Table 3: Installed Locations of CSAV for Linux Documentation Files – CSAV-docs Package**

Path	Description
/etc/csav/email.cfg	A sample e-mail notification file. This file can be used when <b>-notify=user@domain</b> is provided. <b>Note:</b> Administrators can use a text editor to change the content of <b>email.cfg</b> to fit their needs.
/usr/doc/csav/distrib.txt	This file provides contact information about all of the Command AntiVirus distributors.
/usr/doc/csav/readme.txt	The readme file for Command AntiVirus for Linux. This file contains important last-minute information about the functioning of the product.
/usr/doc/csav/legal.txt	This file contains legal information on product copyright, licensing, usage, etc.
/usr/doc/csav/cssunix.pdf	The <i>Command AntiVirus for Unix User's Guide</i> .
/usr/doc/csav/guide.txt	The <i>Command AntiVirus for Unix User's Guide</i> short form in text format.

## TESTING COMMAND ANTIVIRUS

After installing Command AntiVirus, you may want to test its functionality. A file called **eicar.com** is provided for this purpose on the Command web site and needs to be downloaded in order to perform the test. Eicar.com is a test file created by the European Institute for Computer Anti-Virus Research. You can use it to test if CSAV is operating properly. Eicar.com is also useful in demonstrating how Command AntiVirus responds when it finds a virus.

To test Command AntiVirus, just scan **eicar.com**. A message containing the following phrase should appear on-screen:

Infection: EICAR\_Test\_File

This message assures you that Command AntiVirus is functioning properly. If you do not receive this message, then Command AntiVirus is not functioning properly and you will need to troubleshoot the cause of the problem.

## UPDATING COMMAND ANTIVIRUS FOR LINUX

---

The following section contains information on installing an updated version of Command AntiVirus for Linux.



**NOTE:** If you are updating from a version prior to 4.62.0, we recommend that you first uninstall the older version. For more information refer to **Removing Command AntiVirus** located later in this chapter.

Once you have removed the older version, use the installation instructions for a first-time installation. For more information refer to **Installing** located previously in this chapter.

To update an existing version of Command AntiVirus for Linux, follow these steps:

1. At the Linux command prompt, \$, type the following, and press **Enter**:

**su**

The system displays the **Password:** prompt.



2. Type your root password and press **Enter**.
3. To install the Command AntiVirus package, at the command prompt, **#**, type the following, and press **Enter**:

```
rpm -U csav-4.70.0-shared.i386.rpm
```



**NOTE:** We highly recommend that you update the virus definition files (deffiles) at this time. Go to **Step 3 of Updating the Definition Files** to update the deffiles and to complete the updating of Command AntiVirus for Linux.

If you do not want to update the deffiles at this time, go to **Step 4** to complete the installation of the updated version.

4. To complete the updating, at the command prompt, type the following, and press **Enter**:

```
exit
```

The system returns to the Linux command prompt, **\$**.

## UPDATING THE DEFINITION FILES

---

The following section contains information on updating the virus definition files (deffiles). For information on scheduling deffile updates, refer to **Scheduling Updates** located later in this section.

To update the Command AntiVirus for Linux deffiles, follow these steps:

1. At the Linux command prompt, **\$**, type the following, and press **Enter**:

```
su
```

The system displays the **Password:** prompt.

2. Type your root password and press **Enter**.

3. To install the deffiles package, at the command prompt, **#**, type the following, and press **Enter**:

```
rpm -U <deffile_loc/>deflinux.rpm
```



**NOTE:** Replace the **<deffile\_loc/>** with the location of the deffiles.

4. To complete the updating, at the command prompt, type the following, and press **Enter**:

```
exit
```

The system returns to the Linux command prompt, **\$**.

## SCHEDULING UPDATES

If you are a registered user of Command AntiVirus and you have a user name and password, you can schedule deffile updates through **cron**. Use the following command line:

```
5 0 * * * /bin/rpm -U ftp://<user:password>@ftp.commandcom.com/products/commercial/def/deflinux.rpm
```



**NOTE:** Replace the **<user:password>** with your user name:password.

## PERFORMING A VIRUS SCAN

---

To perform a scan for viruses, at the command line, type the following, and press **Enter**:

```
csav -disinf /usr/bin /usr/doc
```

Command AntiVirus begins scanning your **/usr/bin** and **/usr/doc** directories. Entering the path name immediately after **csav** allows you to scan specific directories. Subdirectories are scanned by default.

You can scan more than one directory at a time. In the command stated above, the **/usr/bin** and **/usr/doc** paths are scanned because their path names, which must be separated by a space, have been added to the command line immediately after **csav**. If an infected file is detected, the **-disinf** switch instructs Command AntiVirus to disinfect the file automatically.

## COMMAND-LINE OPTIONS

There are many command-line options (switches) that you can use with Command AntiVirus for Linux. Using these switches requires the following syntax:

```
csav {command-line options} {path}+
```

In the previous syntax:

**csav** is the Command AntiVirus executable

**{command-line options}** can be any of the switches listed in **Table 4** located later in this chapter.

**{path} +** is one or more paths

For example, to scan all files in a directory called **doc**, you can use the following command:

```
csav -disinf /usr/doc/
```

Some examples of **csav** using command-line options are:

```
csav /bin/
csav -list /bin
csav -packed /usr/doc
csav -paranoid /doc -type
csav -report=myrep.txt /doc
```


**Table 4: CSAV for Linux Command-line Switches**

Switch	Description
-all	Scans all files.
-append	Adds to the existing report file. This switch allows you to receive an extended report of what was scanned. If you use the <b>-list</b> switch, this report can become very large so you will need to clear it frequently. The <b>-append</b> switch <b>must</b> be used with the <b>-report</b> switch.
-archive	Scans inside <b>.zip</b> , <b>.cab</b> , <b>.tar</b> , <b>.gz</b> , <b>.rar</b> , <b>.lzh</b> and <b>.arj</b> files.
-collect	Scans a virus collection.
-delete	Deletes infected files.
-disinf	Disinfects when possible. Deletes first-generation samples and files destroyed by overwriting viruses. It will never delete a file that can be disinfected.
-dumb	Scans all files. This switch is to be used with the <b>-collect</b> switch.
-follow	Follows symbolic links.

Table 4: CSAV for Linux Command-line Switches

Switch	Description
-help	Displays this list of switches.
-list	Lists all files being scanned.
-nobreak	Does not abort the scan if the <b>Ctrl-C</b> key combination is pressed.
-noheur	Disables heuristic scanning abilities.
-nosub	Does not scan subdirectories.
-notify=user@domain.com	When a virus is detected, send an e-mail to the designated address (replace <b>user@domain.com</b> with a legitimate e-mail address).
-packed	Unpacks compressed executables.
-quarantine=<directory name>	Quarantines the infected files to the directory specified at the command line. <b>Important:</b> Only users with root permissions can use this command-line option.
-rename	Renames infected <b>com/exe</b> files to <b>vom/vxe</b> .
-report=	Sends the output to a specified file.
-removeall	Removes all macros from all documents.
-removenew	Removes new variants of macro viruses by removing all macros from infected documents.
-saferemove	Removes all macros from all documents if a known virus is detected.
-silent	Does not generate any screen output.
-syslog	Logs all detected infections into the system log (usually /var/log/messages). <b>Important:</b> Only the root is allowed to use this switch as it generates additional output to the system files.

**Table 4: CSAV for Linux Command-line Switches**

Switch	Description
-virlist	<p>If specified, displays the virus list on the screen. If used, this switch <b>must</b> be the <b>only</b> option. Use redirection to save the virus list as a file. For example:</p> <pre data-bbox="596 396 1026 418">csav -virlist &gt; virlist.lis</pre> <p>To view the virus list one screen at a time, you can use the <b> more</b> command:</p> <pre data-bbox="588 516 892 539">csav -virlist  more</pre>
-virno	Counts the known viruses.
	<p>The following switches are non-functional in Command AntiVirus for Linux: <b>-hard</b>, <b>-inter</b>, <b>-noboot</b>, <b>-nofile</b>, <b>-nofloppy</b>, <b>-nomem</b>, <b>-page</b>, and <b>-wrap</b>.</p>

## E-mail Notification

Command AntiVirus for Linux can be configured to send a virus notification e-mail message to a specific address. For example, when a virus is detected, an e-mail notification containing important information about the infection can be sent to a company's MIS department.

To enable e-mail notification, you must use the **-notify=user@domain.com** command-line switch (see **Table 4** located previously in this chapter). The default notification message is located in the **email.cfg** file. The default message is:

Dear Sir/Madam,

On %DATE% Command AntiVirus version %VER% found the virus %VIRUS% in the file %FILE% (owned by %OWNER%) residing on the machine %MACHINE%.

Regards,

The Administrator



**NOTE:** You can use any standard text editor to reword the notification message to fit your needs.

When the notification message is generated, variables in **email.cfg** are replaced automatically with specific information about those variables. For example, if the **%VIRUS%** variable is used in **email.cfg**, the notification message will contain the name of the virus. A notification generated from the default **email.cfg** will look similar to the following:

Dear Sir/Madam,

On Tue Aug 10 16:03:28 1999 Command AntiVirus version 4.60.0 found the virus W97M/Test Macro in the file 1/macro97.doc (owned by DBanner) residing on the machine hulk017.zigysoft.com.

Regards,

The Administrator

The variables that are available for use in the Command Antivirus virus notification e-mail message are described in the following table:

**Table 5: Notification Message Variables**

Variable	Description
%DATE%	Will be replaced with the current date. This variable reports the current day of the week, the calendar date, and the time of day.
%FILE%	Will be replaced with the name of the infected file.
%MACHINE%	Will be replaced with the machine name as found through DNS.

**Table 5: Notification Message Variables**

Variable	Description
%OWNER%	Will be replaced by the user name of the owner of the infected file. <b>Important:</b> The owner is the account that currently “owns” the file. It is <b>not</b> guaranteed that this account created the file.
%VER%	Will be replaced with the version number of the currently running Command AntiVirus.
%VIRUS%	Will be replaced with the name of the virus infecting the file.

## REMOVING COMMAND ANTIVIRUS

---

To remove Command AntiVirus for Linux, follow these steps:

1. At the Linux command prompt, \$, type the following, and press **Enter**:

```
su
```

The system displays the **Password:** prompt.

2. Type your root password and press **Enter**.
3. To remove the deffiles package, at the command prompt, #, type the following and press **Enter**:

```
rpm -e deffiles
```

4. To remove the Command AntiVirus package, at the command prompt, type the following and press **Enter**:

```
rpm -e csav
```



5. To remove the documentation package, at the command prompt, type the following and press **Enter**:

```
rpm -e csav-docs
```

6. To complete the removal of Command AntiVirus for Linux, at the command prompt, type the following and press **Enter**:

```
exit
```

The system returns to the Linux command prompt, \$.





# CSAV FOR SOLARIS

This chapter provides pre-installation requirements and instructions on installing and removing Command AntiVirus for Solaris™ on both the SPARC® and Intel® platforms. Also included is information on performing virus scans, using the product's command-line switches, and using the Command AntiVirus for Solaris e-mail notification feature.

## PRE-INSTALLATION REQUIREMENTS

---

### SPARC PLATFORM

The system requirements for Command AntiVirus for Solaris on the SPARC platform are:

- A system that is running Solaris 8 or higher
- At least 6.0 MB of available hard disk space

### INTEL PLATFORM

The system requirements for Command AntiVirus for Solaris on the Intel platform are:

- A system that is running Solaris 7 or higher
  - At least 6.0 MB of available hard disk space
-

## INSTALLATION

---

Installing Command AntiVirus for Solaris is easy to do. The installation places all of the required Command AntiVirus files in the necessary directories. Before beginning, please read the installation instructions thoroughly. This will help you to anticipate any choices that you may need to make during the installation process.

Command AntiVirus for Solaris consists of three packages: the Command AntiVirus scan engine, the virus definition files, also referred to as deffiles, and the documentation.



**NOTE:** You can install Command AntiVirus for Solaris through the **pkgadd** command or by using **Admintool**.

The documentation package installs the translated versions of the following:

- **readme.txt** – contains important last-minute information about the functioning of the product.
- **guide.txt** – the short form of the *Command AntiVirus for Unix User's Guide* in text format.
- **distrib.txt** – contains contact information about all of the Command Software distributors.
- **legal.txt** – contains legal information on product copyright, licensing, usage, etc.
- **email.cfg** – a sample e-mail notification file. This file can be used when **-notify=user@domain** is provided.



**NOTE:** Administrators can use a text editor to change the content of **email.cfg** to fit their needs.

- **cssunix.pdf** – the *Command AntiVirus for Unix User's Guide*.



**NOTE:** The English versions of the first five files are installed when you install the Command AntiVirus package. The **cssunix.pdf** file is **not** installed unless you install the documentation package.

## INSTALLING USING THE PKGADD COMMAND

To install Command AntiVirus for Solaris using the **pkgadd** command, follow these steps:

1. At the Solaris command prompt, \$, type the following, and press **Enter**:

```
su
```

The system displays the **Password:** prompt.

2. Type your root password and press **Enter**.
3. Place the CD-ROM containing Command AntiVirus for Solaris into your CD-ROM drive.

**If vold is running** – the system displays a file manager window, and the CD is mounted.

**If vold is not running** – mount the CD manually.



**NOTE:** Vold mounts the CDs on /cdrom/VOLNAME, where VOLNAME is the CD Volume Name.

4. To install the Command AntiVirus scan engine package, at the command prompt, #, type the following, and press **Enter**:

- SPARC Platform

```
pkgadd -d /cdrom/CSAV_x_xx/CSAV/sol/pkg/sparc/CSSlcsav-x.xx.x-sparc.pkg
```

- Intel Platform

```
pkgadd -d /cdrom/CSAV_x_xx/CSAV/sol/pkg/i386/CSSlcsav-x.xx.x-i386.pkg
```

The x\_xx and x.xx.x represent the Command AntiVirus version number, for example 4\_70 and 4.70.0.



**NOTE:** The actual location may vary. It depends on where the CD is mounted and the volume label of the CD.

The system asks if you want to process the package.

5. Press **Enter**, or at the command prompt, type **all** and press **Enter**.

The system asks if you will allow scripts to be executed with super-user privileges. These scripts update links onto your file system and make Command AntiVirus available for all users.

6. At the command prompt, type **y** and press **Enter**.
7. To install the deffiles package, at the command prompt, **#**, type the following, and press **Enter**:

```
pkgadd -d /cdrom/CSAV_x_xx/CSAV/sol/pkg/CSSIdeffl.pkg
```

The **x\_xx** represents the version number, for example 4\_70.



**NOTE:** The actual location may vary. It depends on where the CD is mounted and the volume label of the CD.

The system asks if you want to process the package.

8. Press **Enter**, or at the command prompt, type **all** and press **Enter**.
9. To install the documentation package, at the command prompt, type the following, and press **Enter**:

```
pkg_add -d/cdrom/CSAV/sol/CSSIdocs-x.xx.x-language.pkg
```

The **x.xx.x** represents the Command AntiVirus version number, for example, 4.70.0. The **language** represents the language used, for example, **english**.

The system asks if you want to process the package.

10. Press **Enter**, or at the command prompt, type **all** and press **Enter**.



**NOTE:** The actual location may vary. It depends on where the CD is mounted and the volume label of the CD.

11. To complete the installation of Command AntiVirus for Solaris, at the command prompt, type the following, and press **Enter**:

**exit**

The system returns to the Solaris command prompt, \$.

## Verifying the Pkgadd Installation

To verify that the Command AntiVirus scan engine package is installed properly, at the command prompt, \$, type the following and press **Enter**:

**pkginfo CSSIcsav**

The system displays the following message:

```
system    CSSIcsav      Command AntiVirus for Solaris
```

To verify that the definition files package is installed properly, at the command prompt, \$, type the following and press **Enter**:

**pkginfo CSSIdeffl**

The system displays the following message:

```
system    CSSIdeffl     Definition Files for Solaris
```

To verify that the documentation package is installed properly, at the command prompt, \$, type the following and press **Enter**:

**pkginfo CSSIdocs**

The system displays the following message:

```
system    CSSIdocs      Command Software AntiVirus for
                        Solaris supporting documentation
```

For more information, refer to the manual page of pkginfo.

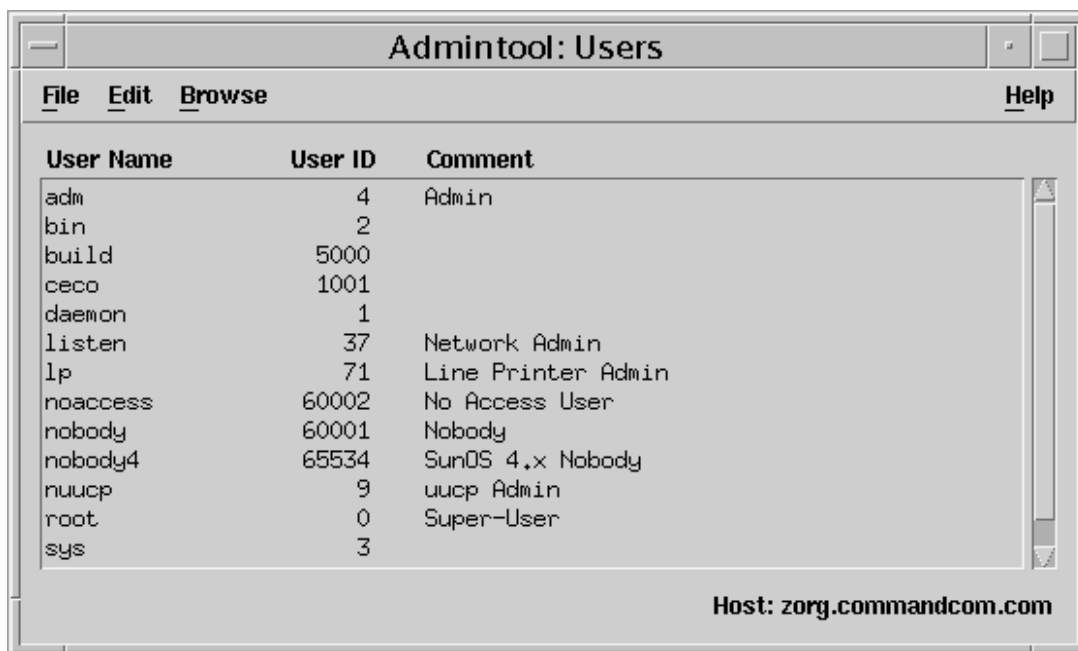
## INSTALLING USING ADMINTOOL



**NOTE:** Before you begin the installation, make sure that you have root permissions.

To install Command AntiVirus for Solaris using **Admintool**, follow these steps:

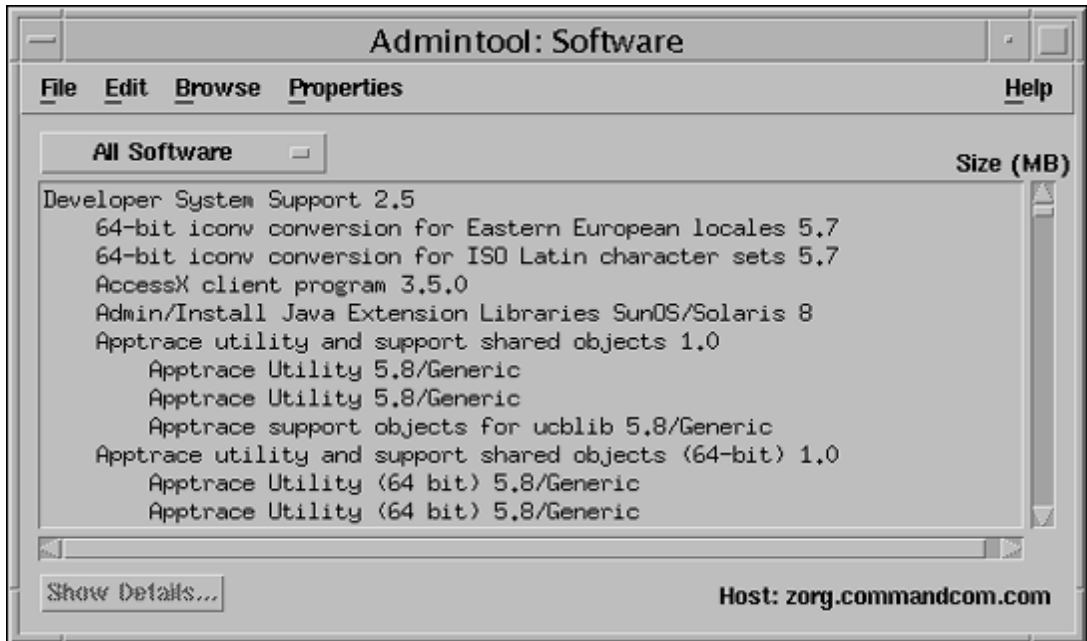
1. At the command prompt, **#**, start **Admintool** by typing **admintool&** and pressing **Enter**. The system displays the **Admintool: Users** dialog box:



**Admintool: Users Dialog Box**



2. On the menu bar, click **Browse** and then **Software**. The system displays the **Admintool: Software** dialog box:



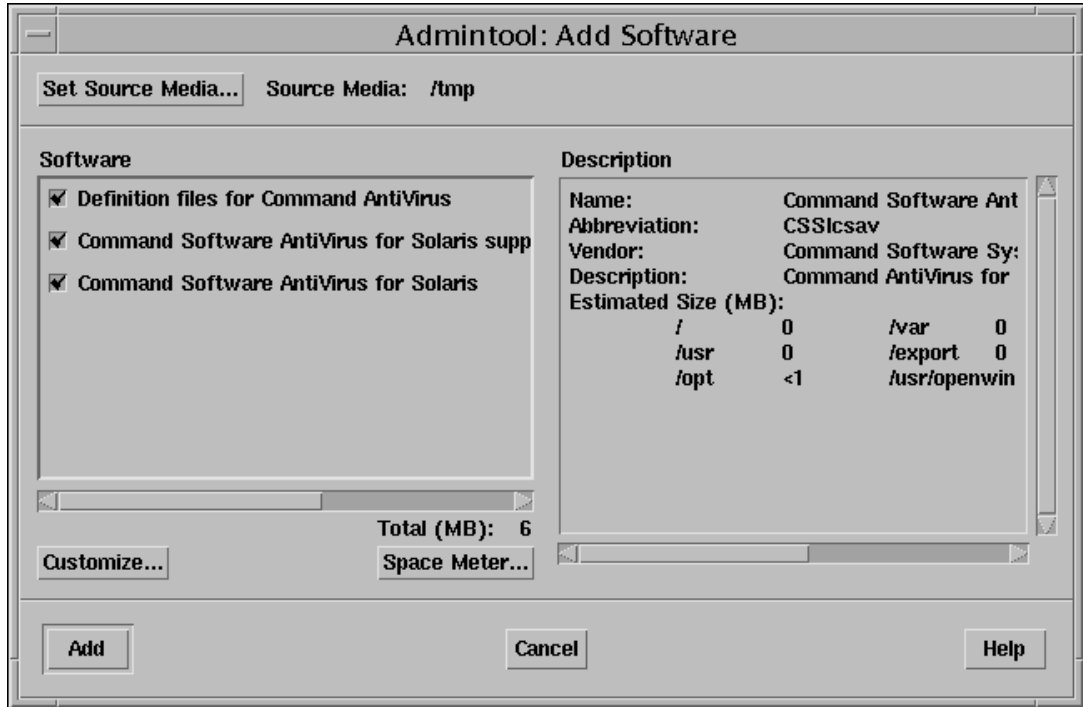
Admintool: Software Dialog Box

3. On the menu bar, click **Edit** and then **Add**. The system displays the **Admintool: Set Source Media** dialog box:



**Admintool: Set Source Media Dialog Box**

4. In the **Software Location** list, select **one** of the following:
  - **CD with volume management** - if installing from CDROM (vold running).
  - **CD without volume management** -if installing from CDROM (vold is not running. Make sure CD is mounted).
  - **Hard Disk** - if installing from directory onto hard disk.
5. In the **Directory** text box, type the path of where the software resides.
6. Click **OK**. The system displays the **Admintool: Add Software** dialog box:



Admintool: Add Software Dialog Box

7. Select the **Command Software AntiVirus for Solaris** and **Definition files for Command AntiVirus** check boxes. If you want to install the documentation, select **Documentation for Command AntiVirus** check box. Installing documentation is optional.



To ensure that Command AntiVirus functions properly, both the **Command Software AntiVirus for Solaris** and **Definition files for Command AntiVirus** check boxes **must** be selected.

8. Click **Add**. The installation begins.

During the installation the system asks if you will allow scripts to be executed with super-user privileges. These scripts update links onto your file system and make Command AntiVirus available for all users.

- At the command prompt, type **y** and press **Enter**.

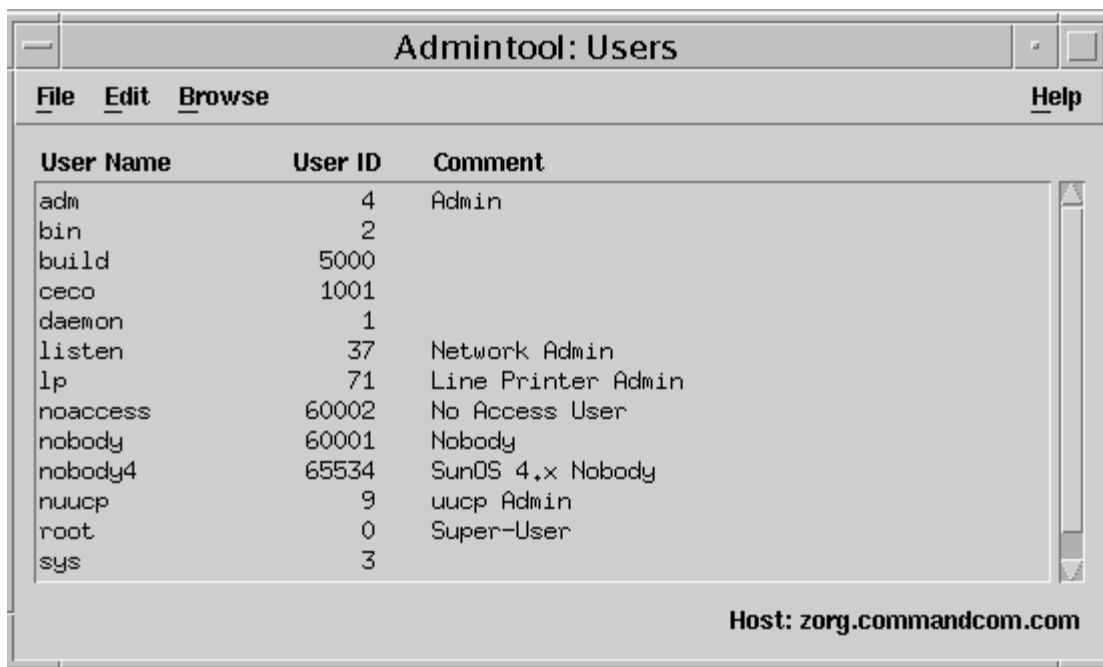
The system notifies you that the installation was successful.

- Press **Enter**. The system returns to the **Admintool: Add Software** dialog box.
- Click **Cancel** to exit **Admintool**.

## Verifying the Admintool Installation

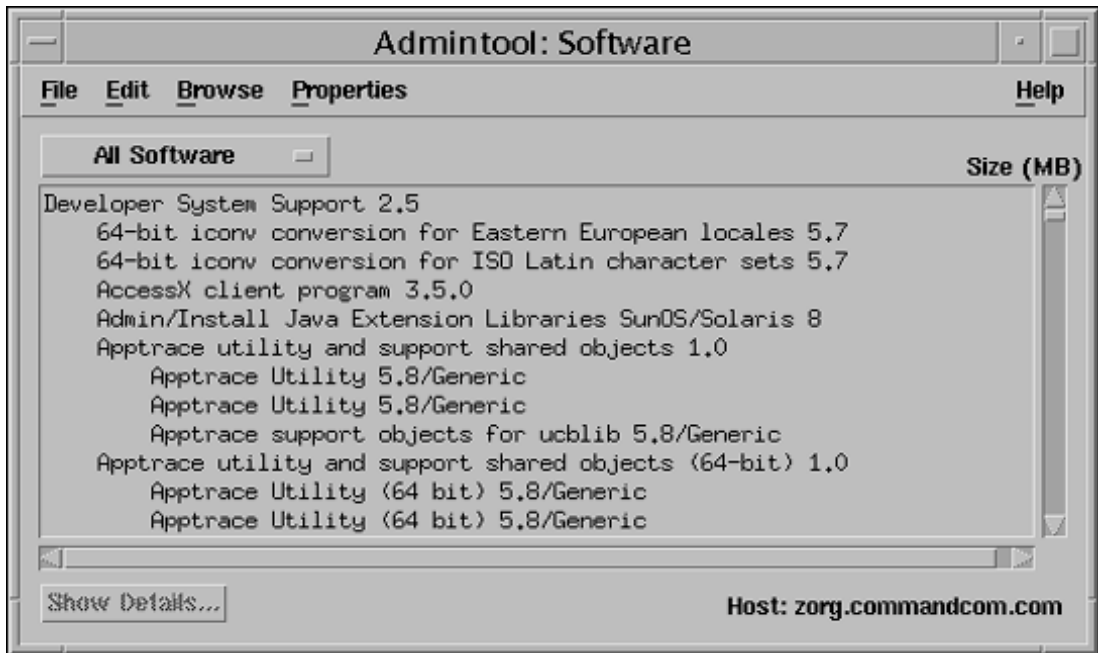
To verify that Command AntiVirus is installed properly follow these steps.

- At the command prompt, **#**, start **Admintool** by typing **admintool&** and pressing **Enter**. The system displays the **Admintool: Users** dialog box:



**Admintool: Users Dialog Box**

- On the menu bar, click **Browse** and then **Software**. The system displays the **Admintool: Software** dialog box:



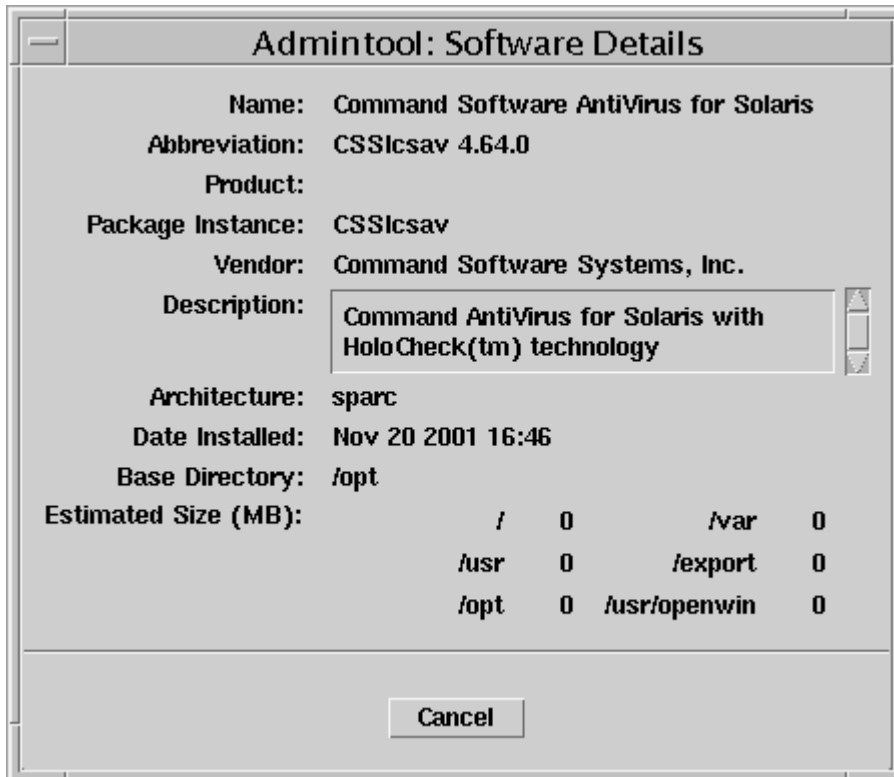
Admintool: Software Dialog Box

3. Click the **All Software** button, and select **System Software**.
4. Scroll through the list to locate and select **Command Software AntiVirus for Solaris**.



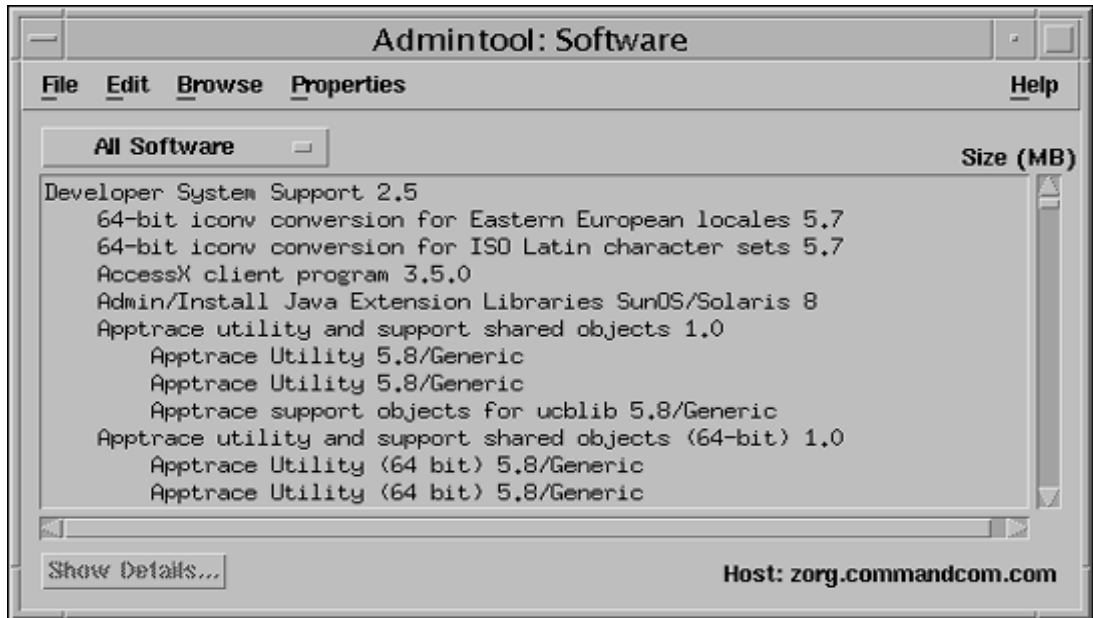
**NOTE:** If **Command Software AntiVirus for Solaris** is not listed, the installation was not successful.

5. Click **Show Details**. The system displays the **Admintool: Software Details** dialog box:



Admintool: Software Details Dialog Box

- Click **Cancel**. The system returns to the **Admintool: Software** dialog box:



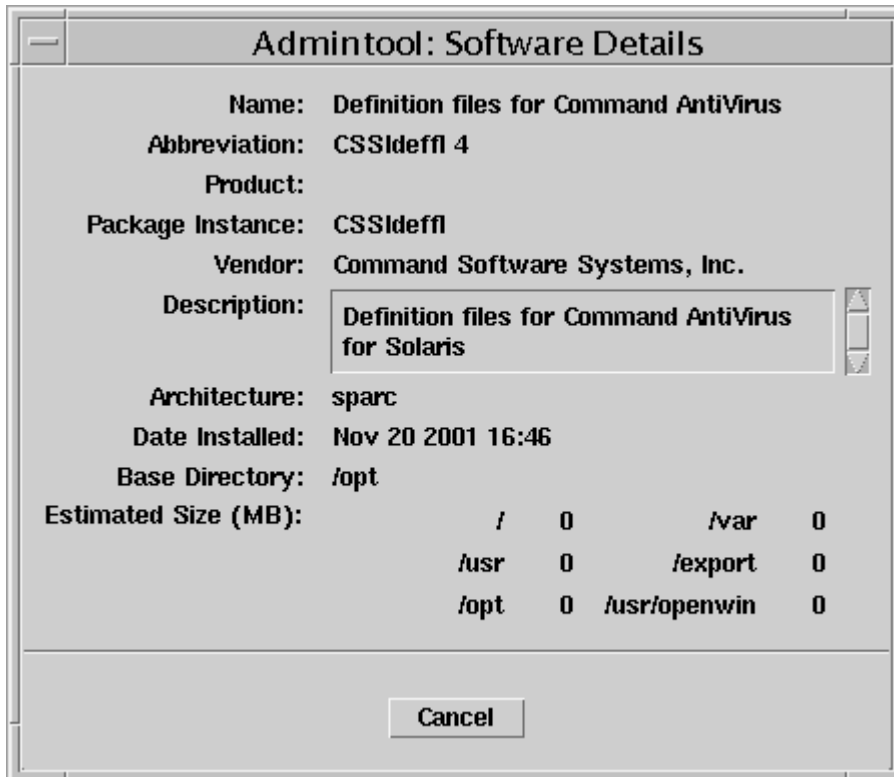
Admintool: Software Dialog Box

7. Click the **All Software** button, and select **System Software**.
8. Scroll through the list to locate and select **Definition files for Command AntiVirus**.



**NOTE:** If **Definition files for Command AntiVirus** is not listed, the installation was not successful.

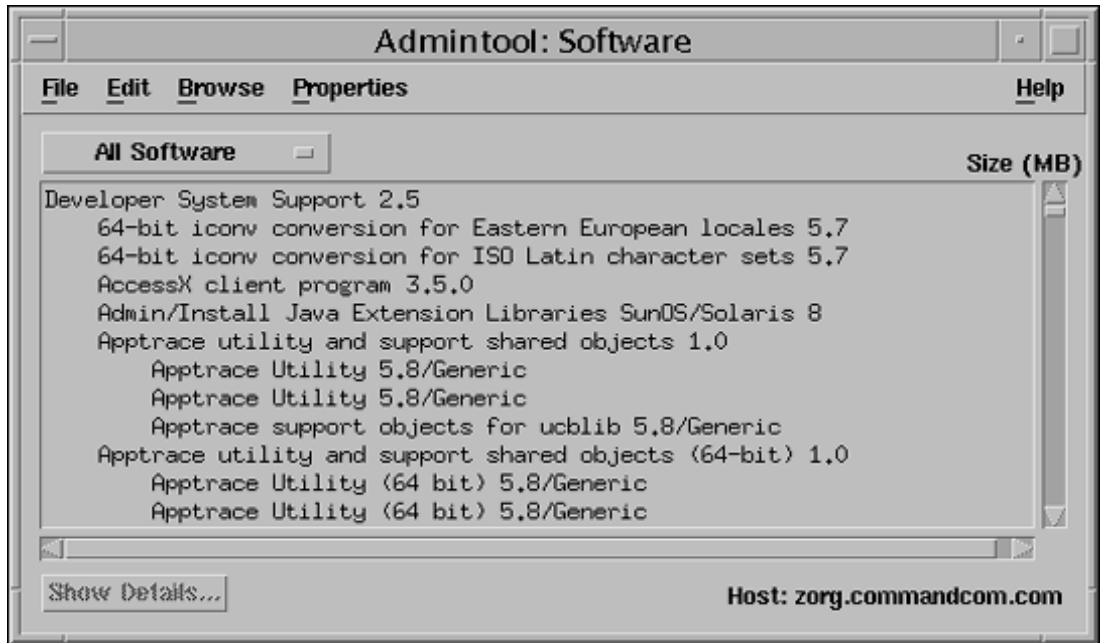
9. Click **Show Details**. The system displays the **Admintool: Software Details** dialog box:



Admintool: Software Details Dialog Box

- Click **Cancel**. The system returns to the **Admintool: Software** dialog box.





Admintool: Software Dialog Box

11. Click the **All Software** button, and select **System Software**.
12. Scroll through the list to locate and select **Documentation for Command AntiVirus**.



**NOTE:** If **Documentation for Command AntiVirus** is not listed, the installation was not successful.

13. Click **Show Details**. The system displays the **Admintool: Software Details** dialog box:



**Admintool: Software Details Dialog Box**

14. Click **Cancel**. The system returns to the **Admintool: Software** dialog box.
15. Click the **Close** button on the tool bar to exit **Admintool**.

## LOCATION OF INSTALLED FILES

For updating or troubleshooting purposes, you may need to know the location of the Command AntiVirus files (**CSSIcsav** package), the virus definition files (**CSSIdeffl** package), and the documentation (**CSSIdocs** package) that are installed on your system. For example, when you update the **macro.def**, **sign2.def**, and **sign.def** files (**CSSIdeffl** package), you may need to know their locations.

CSAV for Solaris installs under the **/opt/CSSIcsav** directory. Several symbolic links that enable Command AntiVirus to function properly are created in some system directories. **Table 1** and **Table 2** provide the locations of all the files and the symbolic links that are installed through the three packages.

**Table 1: Installed Locations of CSAV for Solaris Files – CSSIcsav Package**

Path	Description
/usr/bin/csav Link to: /opt/CSSIcsav/bin/csav	The Command AntiVirus command-line scanner.
/usr/lib/libcscan.so Link to: /opt/CSSIcsav/lib/libcscan.so.x.xx	A symbolic link to the most recently installed core scan engine shared library.
/opt/CSSIcsav/lib/libcscan.so.x.xx	The core scan engine shared library used by CSAV. The <b>x.xx</b> represents the version number of the product, for example, <b>4.70</b> . <b>Note:</b> The <b>/usr/lib/libcscan.so</b> path mentioned above links to this specific file.
/etc/csav Link to: /opt/CSSIcsav/etc	The file placeholder and definition file placeholder.
/opt/CSSIcsav/etc/english.tx1	The file containing language-specific text.

**Table 1: Installed Locations of CSAV for Solaris Files – CSSIcsav Package**

Path	Description
/opt/CSSIcsav/etc/email.cfg	A sample e-mail notification file. This file can be used when <b>-notify=user@domain</b> is provided. <b>Note:</b> Administrators can use a text editor to change the content of <b>email.cfg</b> to fit their needs.
/opt/CSSIcsav/Docs/distrib.txt	This file provides contact information about all of the Command AntiVirus distributors.
/opt/CSSIcsav/Docs/readme.txt	The readme file for Command AntiVirus for Solaris. This file contains important last-minute information about the functioning of the product.
/opt/CSSIcsav/Docs/legal.txt	This file contains legal information on product copyright, licensing, usage, etc.
/opt/CSSIcsav/Docs/guide.txt	The <i>Command AntiVirus for Unix User's Guide</i> short form in text format.

**Table 2: Installed Locations of CSAV for Solaris Definition Files – CSSIdeffl Package**

Path	Description
/opt/CSSIcsav/etc/macro.def	The virus signature definition file for macro viruses.
/opt/CSSIcsav/etc/sign.def	The virus signature definition file for non-macro viruses.
/opt/CSSIcsav/etc/sign2.def	The virus signature extended definition file.

**Table 3: Installed Locations of CSAV for Solaris Documentation Files – CSSIdocs Package**

Path	Description
/opt/CSSlcsav/etc/email.cfg	A sample e-mail notification file. This file can be used when <b>-notify=user@domain</b> is provided. <b>Note:</b> Administrators can use a text editor to change the content of <b>email.cfg</b> to fit their needs.
/opt/CSSlcsav/Docs/distrib.txt	This file provides contact information about all of the Command AntiVirus distributors.
/opt/CSSlcsav/Docs/readme.txt	The readme file for Command AntiVirus for Solaris. This file contains important last-minute information about the functioning of the product.
/opt/CSSlcsav/Docs/legal.txt	This file contains legal information on product copyright, licensing, usage, etc.
/opt/CSSlcsav/Docs/cssunix.pdf	The <i>Command AntiVirus for Unix User's Guide</i> .
/opt/CSSlcsav/Docs/guide.txt	The <i>Command AntiVirus for Unix User's Guide</i> short form in text format.

## TESTING COMMAND ANTIVIRUS

After installing Command AntiVirus, you may want to test its functionality. A file called **eicar.com** is provided for this purpose on the Command web site and needs to be downloaded in order to perform the test. Eicar.com is a test file created by the European Institute for Computer Anti-Virus Research. You can use it to test if CSAV is operating properly. Eicar.com is also useful in demonstrating how Command AntiVirus responds when it finds a virus.

To test Command AntiVirus, just scan **eicar.com**. A message containing the following phrase should appear on-screen:

Infection: EICAR\_Test\_File

This message assures you that Command AntiVirus is functioning properly. If you do not receive this message, then Command AntiVirus is not functioning properly and you will need to troubleshoot the cause of the problem.

## UPDATING THE DEFINITION FILES

---

The following section contains information on updating the virus definition files (deffiles).



**NOTE:** Before you begin the update, make sure that you have root permissions.

To update the Command AntiVirus for Solaris deffiles, follow these steps:

1. At the command prompt, **#**, type the following, and press **Enter**:

```
pkgadd -d <deffile_loc/>CSSIdeffl.pkg
```



**NOTE:** Replace the **<deffile\_loc/>** with the location of the deffiles.

The system asks if you want to process the package.

2. Press **Enter**, or at the command prompt, type **all** and press **Enter**.

3. To complete the deffiles package update, at the command prompt, type the following and press **Enter**:

```
exit
```

The system returns to the Solaris command prompt, \$.

## Verifying the Pkgadd Update Installation

To verify that the definition files (deffiles) update package is installed properly, at the command prompt, \$, type the following and press **Enter**:

```
pkginfo CSSIdeffl
```

The system displays the following message:

```
system  CSSIdeffl  Definition Files for Solaris
```

For more information, refer to the manual page of pkginfo.

## PERFORMING A VIRUS SCAN

---

To perform a scan for viruses, at the command line, type the following, and press **Enter**:

```
csav -disinf /usr/bin /usr/doc
```

Command AntiVirus begins scanning your **/usr/bin** and **/usr/doc** directories. Entering the path name immediately after **csav** allows you to scan specific directories. Subdirectories are scanned by default.

You can scan more than one directory at a time. In the command stated above, the **/usr/bin** and **/usr/doc** paths are scanned because their path names, which must be separated by a space, have been added to the command line immediately after **csav**. If an infected file is detected, the **-disinf** switch instructs Command AntiVirus to disinfect the file automatically.

## COMMAND-LINE OPTIONS

There are many command-line options (switches) that you can use with Command AntiVirus for Solaris. For more information, refer to the on-line manual page (man csav). Using these switches requires the following syntax:

```
csav {command-line options} {path}+
```

In the above syntax:

**csav** is the Command AntiVirus executable

**{command-line options}** can be any of the switches listed in **Table 4** located later in this chapter.

**{path}+** is one or more paths

For example, to scan all files in a directory called **doc**, you can use the following command:

```
csav -disinf /usr/doc/
```

Some examples of **csav** using command-line options are:

```
csav /bin/
```

```
csav -list /bin
```

```
csav -packed /usr/doc
```

```
csav -paranoid /doc -type
```

```
csav -report=myrep.txt /doc
```


If you do not provide at least one command-line option, **csav** exits.



Table 4: CSAV for Solaris Command-line Switches

Switch	Description
-all	Scans all files.
-append	Adds to the existing report file. This switch allows you to receive an extended report of what was scanned. If you use the <b>-list</b> switch, this report can become very large so you will need to clear it frequently. The <b>-append</b> switch <b>must</b> be used with the <b>-report</b> switch.
-archive	Scans inside <b>.zip</b> , <b>.cab</b> , <b>.tar</b> , <b>.gz</b> , <b>.rar</b> , <b>.lzh</b> and <b>.arj</b> files.
-collect	Scans a virus collection.
-delete	Deletes infected files.
-disinf	Disinfects when possible. Deletes first-generation samples and files destroyed by overwriting viruses. It never deletes a file that can be disinfected.
-dumb	Scans all files. This switch is to be used with the <b>-collect</b> switch.
-follow	Follows symbolic links.
-help	Displays this list of switches.
-list	Lists all files being scanned.
-nobreak	Does not abort the scan if the <b>Ctrl-C</b> key combination is pressed.
-noheur	Disables heuristic scanning abilities.
-nosub	Does not scan subdirectories.
-notify=user@domain.com	When a virus is detected, sends an e-mail to the designated address (replace <b>user@domain.com</b> with a legitimate e-mail address).
-packed	Unpacks compressed executables.

Table 4: CSAV for Solaris Command-line Switches

Switch	Description
-quarantine=<directory name>	Quarantines the infected files to the directory specified at the command line. <b>Important:</b> Only users with root permissions can use this command-line option.
-rename	Renames infected <b>com/exe</b> files to <b>vom/vxe</b> .
-report=	Sends the output to a specified file.
-removeall	Removes all macros from all documents.
-removenew	Removes new variants of macro viruses by removing all macros from infected documents.
-saferemove	Removes all macros from all documents if a known virus is detected.
-silent	Does not generate any screen output.
-syslog	Logs all detected infections into the system log. Only the root is allowed to use this switch as it generates additional output to the system files.
-virlist	If specified, displays the virus list on the screen. If used, this switch <b>must</b> be the <b>only</b> option. Use redirection to save the virus list as a file. For example:  <pre>csav -virlist &gt; virlist.lis</pre> <p>To view the virus list one screen at a time, you can use the <b> more</b> command:</p> <pre>csav -virlist  more</pre>
-virno	Counts the known viruses.
	The following switches are non-functional in Command AntiVirus for Solaris: <b>-hard</b> , <b>-inter</b> , <b>-noboot</b> , <b>-nofile</b> , <b>-nofloppy</b> , <b>-nomem</b> , <b>-page</b> , and <b>-wrap</b> .

## E-mail Notification

Command AntiVirus for Solaris can be configured to send a virus notification e-mail message to a specific address. For example, when a virus is detected, an e-mail notification containing important information about the infection can be sent to a company's MIS department.

To enable e-mail notification, you must use the **-notify=user@domain.com** command-line switch (see **Table 4** located previously in this chapter). The default notification message is located in the **email.cfg** file. The default message is:

Dear Sir/Madam,

On %DATE% Command AntiVirus version %VER% found the virus %VIRUS% in the file %FILE% (owned by %OWNER%) residing on the machine %MACHINE%.

Regards,

The Administrator



**NOTE:** You can use any standard text editor to reword the notification message to fit your needs.

When the notification message is generated, variables in **email.cfg** are replaced automatically with specific information about those variables. For example, if the **%VIRUS%** variable is used in **email.cfg**, the notification message will contain the name of the virus. A notification generated from the default **email.cfg** will look similar to the following:

Dear Sir/Madam,

On Tue Aug 10 16:03:28 1999 Command AntiVirus version 4.60.0 found the virus W97M/Test Macro in the file 1/macro97.doc (owned by DBanner) residing on the machine hulk017.zigysoft.com.

Regards,

The Administrator

The variables that are available for use in the Command Antivirus virus notification e-mail message are described in the following table:

**Table 5: Notification Message Variables**

Variable	Description
%DATE%	Will be replaced with the current date. This variable reports the current day of the week, the calendar date, and the time of day.
%FILE%	Will be replaced with the name of the infected file.
%MACHINE%	Will be replaced with the machine name as found through DNS.
%OWNER%	Will be replaced by the user name of the owner of the infected file. <b>Important:</b> The owner is the account that currently “owns” the file. It is <b>not</b> guaranteed that this account created the file.
%VER%	Will be replaced with the version number of the currently running Command AntiVirus.
%VIRUS%	Will be replaced with the name of the virus infecting the file.

## REMOVING COMMAND ANTIVIRUS

---

Command AntiVirus for Solaris can be uninstalled from the Solaris command prompt or by using Admintool.

### FROM THE COMMAND PROMPT

To remove Command AntiVirus for Solaris from the command prompt, follow these steps.

1. At the Solaris command prompt, \$, type the following, and press **Enter**:

```
su
```

The system displays the **Password:** prompt.

2. Type your root password, and press **Enter**.
3. To remove the definition files package, at the command prompt, #, type the following and press **Enter**:

```
pkgrm CSSIdeffl
```

The system asks if you want to remove the package.

4. Press **Enter**, or at the command prompt, type **y** and press **Enter**.
5. To remove the Command AntiVirus package, at the command prompt, #, type the following, and press **Enter**:

```
pkgrm CSSIcsav
```

The system asks if you want to remove the package.

6. Press **Enter**, or at the command prompt, type **y** and press **Enter**.

The system asks if you will allow scripts to be executed with super-user privileges. These scripts remove links from your file system and completely uninstall Command AntiVirus.

7. At the command prompt, type **y** and press **Enter**.
8. To remove the documentation package, at the command prompt, #, type the following and press **Enter**:

**pkgrm CSSldocs**

The system asks if you want to remove the package.

9. Press **Enter**, or at the command prompt, type **y** and press **Enter**.
10. To complete the uninstall of Command AntiVirus for Solaris, at the command prompt, type the following, and press **Enter**:

**exit**

The system returns to the Solaris command prompt, \$.

## USING ADMINTOOL



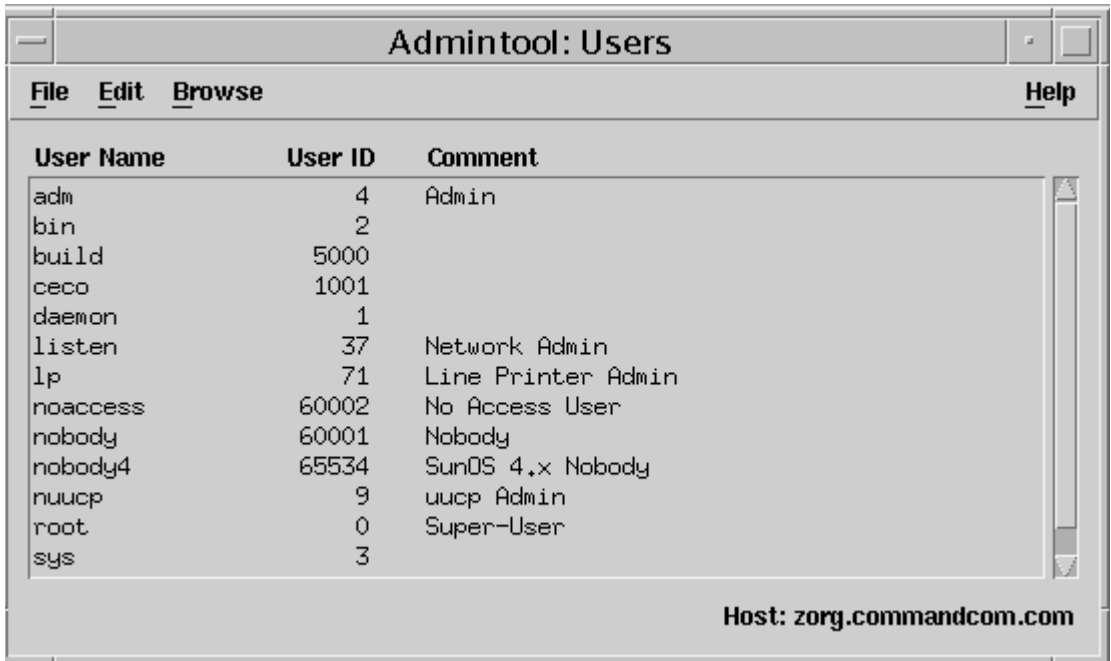
**NOTE:** Before you begin the uninstall, make sure that you have root permissions.



**NOTE:** To properly uninstall Command AntiVirus for Solaris, you must perform the steps to remove Command AntiVirus for Solaris in sequence. Definition files for Command AntiVirus (**CSSideffl**) depend on the Command Software AntiVirus for Solaris (**CSsicsav**) package. You may not be able to uninstall **CSsicsav** until you first uninstall **CSSideffl**. Documentation for Command AntiVirus (**CSldocs**) can be uninstalled at anytime.

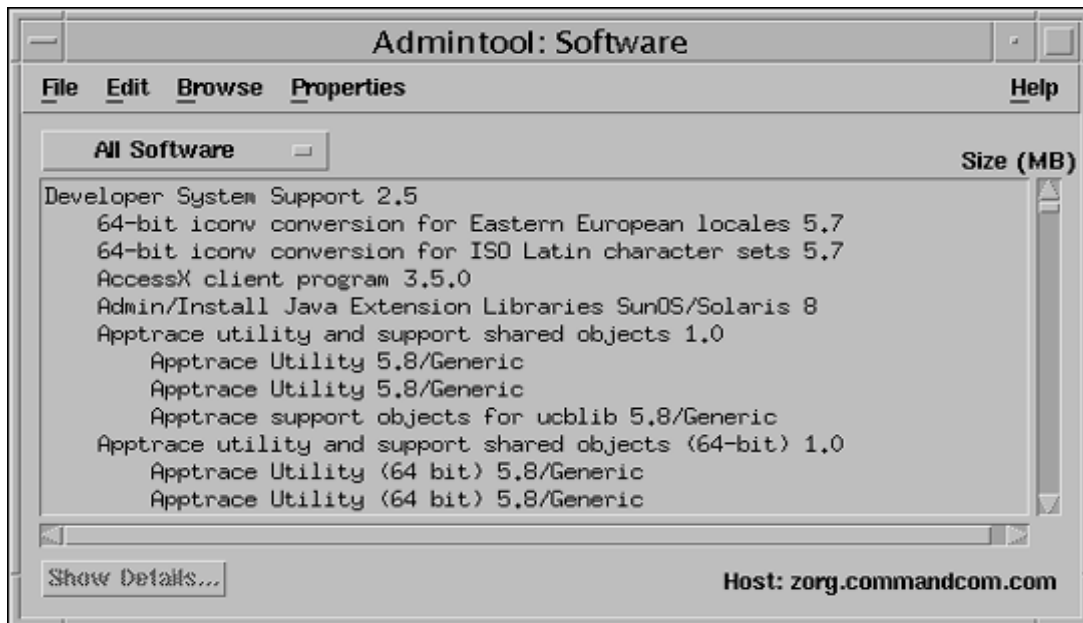
To remove Command AntiVirus for Solaris using Admintool, follow these steps.

1. At the command prompt, start **Admintool** by typing **admintool&** and pressing **Enter**. The system displays the **Admintool: Users** dialog box:



**Admintool: Users Dialog Box**

2. On the menu bar, click **Browse** and then **Software**. The system displays the **Admintool: Software** dialog box:



Admintool: Software Dialog Box

3. Scroll through the list to locate and select **Definition files for Command AntiVirus**.
4. On the menu bar, click **Edit** and then **Delete**. The system displays the **Admintool: Warning** dialog box:





Admintool: Warning Dialog Box

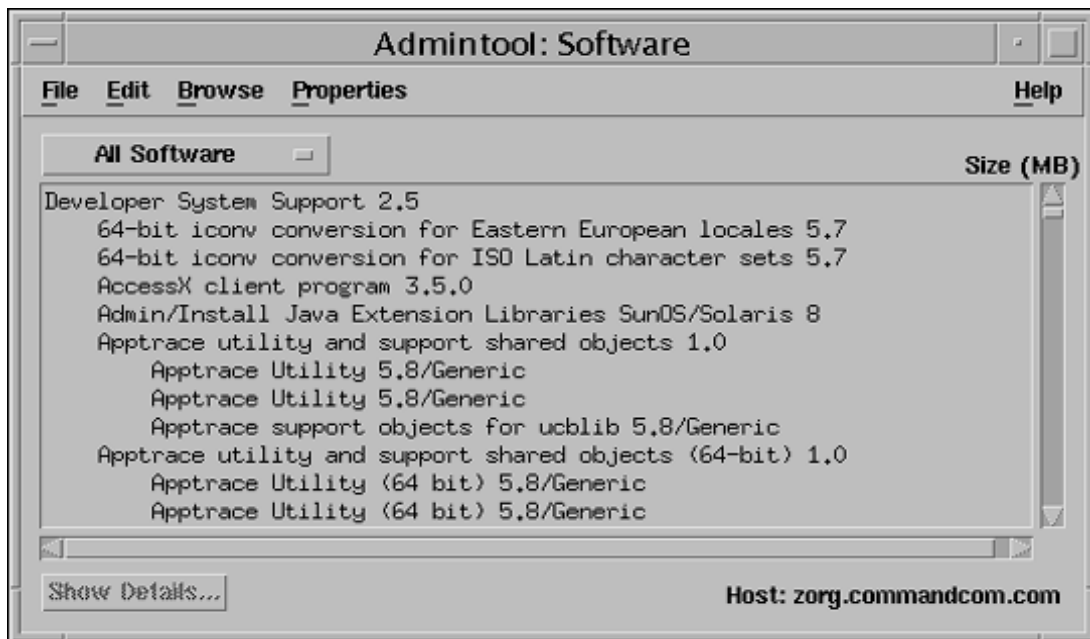
5. Click **Delete**. The system displays the **Admintool: Delete Software** dialog box:



Admintool: Delete Software Dialog Box

You are asked to confirm that you want to remove the package.

6. Type **y**, and press **Enter**. The system returns to the **Admintool: Software** dialog box:



Admintool: Software Dialog Box



**NOTE:** Although the file is deleted, **Definition files for Command AntiVirus** remains in the list until you restart Admintool.

7. Scroll through the list to locate and select **Command Software AntiVirus for Solaris**.
8. On the menu bar, click **Edit** and then **Delete**. The system displays the **Admintool: Warning** dialog box:



Admintool: Warning Dialog Box

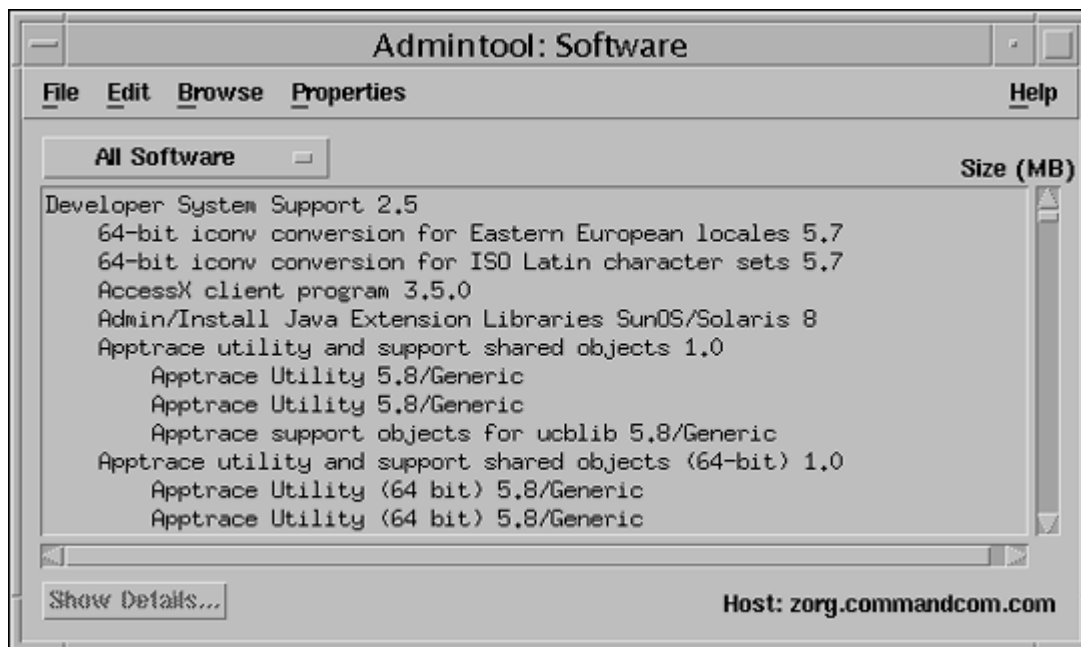
9. Click **Delete**. The system displays the **Admintool: Delete Software** dialog box:



Admintool: Delete Software Dialog Box

You are asked to confirm that you want to remove the package.

10. Type **y** and press **Enter**. The system returns to the **Admintool: Software** dialog box.



**Admintool: Software Dialog Box**



**NOTE:** During the deletion of **Command Software AntiVirus for Solaris**, the system may prompt you one or more times to confirm the deletion of other packages. Type **y** to these prompts.



**NOTE:** Although the file is deleted, **Command Software AntiVirus for Solaris** remains in the list until you restart Admintool.

The removal of Command AntiVirus for Solaris is complete. If you want to uninstall the documentation, proceed to **Step 12**, otherwise continue with **Step 11**.

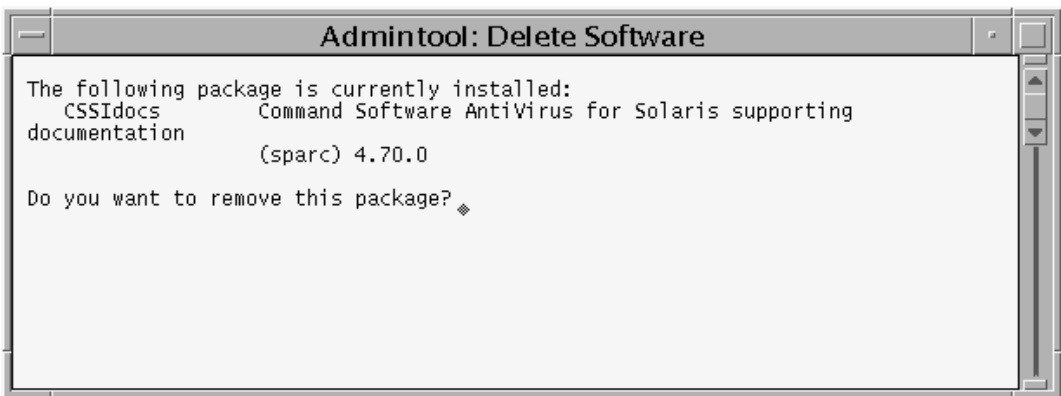
11. Exit the **Admintool: Software** dialog box.

12. Scroll through the list to locate and select **Documentation for Command AntiVirus**.
13. On the menu bar, click **Edit** and then **Delete**. The system displays the **Admintool: Warning** dialog box:



**Admintool: Warning Dialog Box**

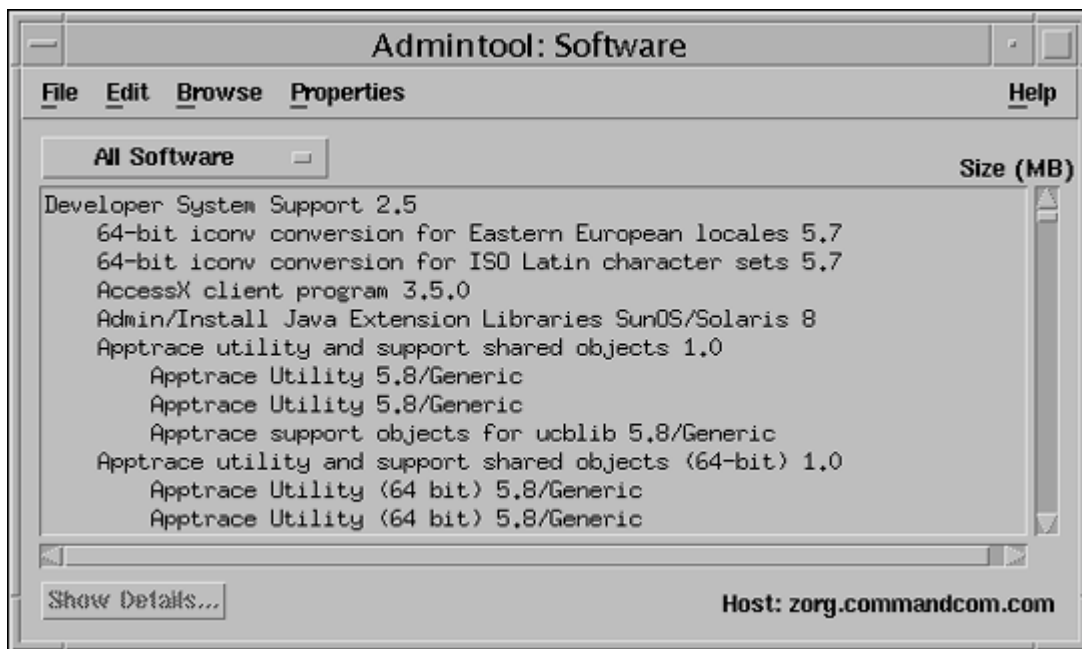
14. Click **Delete**. The system displays the **Admintool: Delete Software** dialog box:



**Admintool: Delete Software Dialog Box**

You are asked to confirm that you want to remove the package.

15. Type **y** and press **Enter**. The system returns to the **Admintool: Software** dialog box:



**Admintool: Software Dialog Box**



**NOTE:** Although the file is deleted, **Documentation for Command AntiVirus** remains in the list until you restart Admintool.

The removal of Documentation for Command AntiVirus is complete.

16. Exit the **Admintool: Software** dialog box.



# CSAV FOR FREEBSD

## PRE-INSTALLATION REQUIREMENTS

---

The system requirements for Command AntiVirus for FreeBSD are:

- An IBM®-compatible computer with a 386 or higher CPU
- FreeBSD 3.5.1 or higher
- At least 4.0 MB of available hard disk space

## INSTALLING

---

Installing Command AntiVirus for FreeBSD is easy to do. The installation places all of the required CSAV files in the necessary directories.

Before beginning, please read the installation instructions thoroughly. This will help you to anticipate any choices that you may need to make during the installation process.

Command AntiVirus for FreeBSD consists of three packages: the Command AntiVirus scan engine, the virus definition files also referred to as deffiles, and the documentation.

---

The documentation package installs the translated versions of the following:

- **readme.txt** – contains important last-minute information about the functioning of the product.
- **guide.txt** – the short form of the *Command AntiVirus for Unix User's Guide* in text format.
- **distrib.txt** – contains contact information about all of the Command Software distributors.
- **legal.txt** – contains legal information on product copyright, licensing, usage, etc.
- **email.cfg** – a sample e-mail notification file. This file can be used when **-notify=user@domain** is provided.



**NOTE:** Administrators can use a text editor to change the content of **email.cfg** to fit their needs.

- **cssunix.pdf** – the *Command AntiVirus for Unix User's Guide*.



**NOTE:** The English versions of the first five files are installed when you install the Command AntiVirus package. The **cssunix.pdf** file is **not** installed unless you install the documentation package.

To install Command AntiVirus for FreeBSD, follow these steps:

1. At the FreeBSD command prompt, **\$**, type the following, and press **Enter**:

**su**

The system displays the **Password:** prompt.

2. Type your root password and press **Enter**.



3. At the command prompt, **#**, type the following, and press **Enter**:

```
mount /cdrom
```

4. To install the Command AntiVirus package, at the command prompt, type the following, and press **Enter**:

```
pkg_add /cdrom/CSAV/freebsd/csav-x.xx.x-shared.tgz
```

The **x.xx.x** represents the Command AntiVirus version number, for example, 4.70.0.

5. To install the deffiles package, at the command prompt, type the following, and press **Enter**:

```
pkg_add /cdrom/CSAV/freebsd/csav/freebsd/deffiles.tgz
```

6. To install the documentation package, at the command prompt, type the following, and press **Enter**:

```
pkg_add /cdrom/CSAV/freebsd/csav-docs-x.xx.x-language.tgz
```

The **x.xx.x** represents the Command AntiVirus version number, for example, 4.70.0. The **language** represents the language used, for example, **english**.

7. To complete the installation of Command AntiVirus for FreeBSD, at the command prompt, type the following, and press **Enter**:

```
exit
```

The system returns to the FreeBSD command prompt, **\$**.

## VERIFYING THE INSTALLATION

To verify that the Command AntiVirus package is installed properly, at the command prompt, **\$**, type the following and press **Enter**:

```
pkg_info |grep csav
```

The system displays the following message:

```
csav      Command AntiVirus(tm) for FreeBSD
```

To verify that the deffiles package is installed properly, at the command prompt, type the following and press **Enter**:

```
pkg_info |grep deffiles
```

The system displays the following message:

```
deffiles  Command AntiVirus(tm) for FreeBSD definition files (deffiles)
```

To verify that the documentation package is installed properly, at the command prompt, **\$**, type the following and press **Enter**:

```
pkg_info |grep csav-docs
```

The system displays the following message:

```
csav-docs Command AntiVirus(tm) for FreeBSD supporting documentation
```

## LOCATION OF INSTALLED FILES

For updating or troubleshooting purposes, you may need to know the location of the Command AntiVirus files that were installed on your system. For example, when you update the **macro.def**, **sign2.def**, and **sign.def** files, you may need to know their locations. **Table 1** and **Table 2** provide the locations for the shared and static package files.

**Table 1: Installed Locations of CSAV for FreeBSD Files – CSAV Package**

Path	Description
/usr/bin/csav	The Command AntiVirus command-line scanner.
/usr/lib/libcscan.so	A symbolic link to the most recently installed shared library.
/usr/lib/libcscan.so.x.xx	The shared library for CSAV. The <b>x.xx.x</b> represents the version number of the product, for example, <b>4.70.0</b> . <b>Note:</b> The <b>/usr/lib/libcscan.so</b> path mentioned above links to this specific file.
/etc/csav/english.tx1	The file containing language-specific text.
/etc/csav/email.cfg	A sample e-mail notification file. This file can be used when <b>-notify=user@domain</b> is provided. <b>Note:</b> Administrators can use a text editor to change the content of <b>email.cfg</b> to fit their needs.
/usr/share/doc/csav/distrib.txt	This file provides contact information about all of the Command AntiVirus distributors.
/usr/share/doc/csav/readme.txt	The readme file for Command AntiVirus for FreeBSD. This file contains important last-minute information about the functioning of the product.
/usr/share/doc/csav/legal.txt	This file contains legal information on product copyright, licensing, usage, etc.
/usr/share/doc/csav/guide.txt	The <i>Command AntiVirus for Unix User's Guide</i> short form in text format.
/usr/share/man/man1/csav.1.gz	The online manual page.

**Table 2: Installed Locations of CSAV for FreeBSD Definition Files – Deffiles Package**

Path	Description
/etc/csav/macro.def	The virus signature definition file for macro viruses.
/etc/csav/sign.def	The virus signature definition file for non-macro viruses.
/etc/csav/sign2.def	The virus signature extended definition file.

**Table 3: Installed Locations of CSAV for FreeBSD Documentation Files – CSAV-docs**

Path	Description
/etc/csav/email.cfg	A sample e-mail notification file. This file can be used when <b>-notify=user@domain</b> is provided. <b>Note:</b> Administrators can use a text editor to change the content of <b>email.cfg</b> to fit their needs.
/usr/share/doc/csav/distrib.txt	This file provides contact information about all of the Command AntiVirus distributors.
/usr/share/doc/csav/readme.txt	The readme file for Command AntiVirus for FreeBSD. This file contains important last-minute information about the functioning of the product.
/usr/share/doc/csav/legal.txt	This file contains legal information on product copyright, licensing, usage, etc.
/usr/share/doc/csav/cssunix.pdf	The <i>Command AntiVirus for Unix User's Guide</i> .
/usr/share/doc/csav/guide.txt	The <i>Command AntiVirus for Unix User's Guide</i> short form in text format.

## TESTING COMMAND ANTIVIRUS

After installing Command AntiVirus, you may want to test its functionality. A file called **eicar.com** is provided for this purpose on the Command web site and needs to be downloaded in order to perform the test. Eicar.com is a test file created by the European Institute for Computer Anti-Virus Research. You can use it to test if CSAV is operating properly. Eicar.com is also useful in demonstrating how Command AntiVirus responds when it finds a virus.

To test Command AntiVirus, just scan **eicar.com**. A message containing the following phrase should appear on-screen:

```
Infection: EICAR_Test_File
```

This message assures you that Command AntiVirus is functioning properly. If you do not receive this message, then Command AntiVirus is not functioning properly and you will need to troubleshoot the cause of the problem.

## UPDATING COMMAND ANTIVIRUS FOR FREEBSD

---

The following section contains information on installing an updated version of Command AntiVirus for FreeBSD.

To update an existing version of Command AntiVirus for FreeBSD, follow these steps:

1. At the FreeBSD command prompt, **\$**, type the following, and press **Enter**:

```
su
```

The system displays the **Password:** prompt.

2. Type your root password and press **Enter**.

3. To install the Command AntiVirus package, at the command prompt, **#**, type the following, and press **Enter**:

```
pkg_update csav-x.xx.x-shared.tgz
```

The **x.xx.x** represents the Command AntiVirus version number, for example, 4.70.0.



**NOTE:** We highly recommend that you update the virus definition files (deffiles) at this time. Go to **Step 3 of Updating the Definition Files** to update the deffiles and to complete the updating of Command AntiVirus for FreeBSD.

If you do not want to update the deffiles at this time, go to **Step 4** to complete the installation of the updated version.

4. To complete the updating, at the command prompt, type the following, and press **Enter**:

```
exit
```

The system returns to the FreeBSD command prompt, **\$**.

## UPDATING THE DEFINITION FILES

---

The following section contains information on updating the virus definition files (deffiles). For information on scheduling deffile updates, refer to **Scheduling Updates** located later in this section.

To update the Command AntiVirus for FreeBSD deffiles, follow these steps:

1. At the FreeBSD command prompt, **\$**, type the following, and press **Enter**:

```
su
```

The system displays the **Password:** prompt.

2. Type your root password and press **Enter**.

3. To install the deffiles package, at the command prompt, **#**, type the following, and press **Enter**:

```
pkg_update deffiles.tgz
```

4. To complete the updating, at the command prompt, type the following, and press **Enter**:

```
exit
```

The system returns to the FreeBSD command prompt, **\$**.

## SCHEDULING UPDATES

If you are a registered user of Command AntiVirus and you have a user name and password, you can schedule deffile updates through **cron**. Use the following command line:

```
5 0 * * * /usr/sbin/pkg_update ftp://<user:password>@ftp.commandcom.com/products/commercial/deffiles.tgz
```



**NOTE:** Replace the **<user:password>** with your user name:password.

## PERFORMING A VIRUS SCAN

---

To perform a scan for viruses, at the command line, type the following, and press **Enter**:

```
csav -disinf /usr/bin /usr/doc
```

Command AntiVirus begins scanning your **/usr/bin** and **/usr/doc** directories. Entering the path name immediately after **csav** allows you to scan specific directories. Subdirectories are scanned by default.

You can scan more than one directory at a time. In the command stated above, the **/usr/bin** and **/usr/doc** paths are scanned because their path names, which must be separated by a space, have been added to the command line immediately after **csav**. If an infected file is detected, the **-disinf** switch instructs Command AntiVirus to disinfect the file automatically.

## COMMAND-LINE OPTIONS

There are many command-line options (switches) that you can use with Command AntiVirus for FreeBSD. Using these switches requires the following syntax:

```
csav {command-line options} {path}+
```

In the previous syntax:

**csav** is the Command AntiVirus executable

**{command-line options}** can be any of the switches listed in **Table 4** located later in this chapter.

**{path} +** is one or more paths

For example, to scan all files in a directory called **doc**, you can use the following command:

```
csav -disinf /usr/doc/
```

Some examples of **csav** using command-line options are:

```
csav /bin/
```

```
csav -list /bin
```

```
csav -packed /usr/doc
```

```
csav -paranoid /doc -type
```


```
csav -report=myrep.txt /doc
```



Table 4: CSAV for FreeBSD Command-line Switches

Switch	Description
-all	Scans all files.
-append	Adds to the existing report file. This switch allows you to receive an extended report of what was scanned. If you use the <b>-list</b> switch, this report can become very large so you will need to clear it frequently. The <b>-append</b> switch <b>must</b> be used with the <b>-report</b> switch.
-archive	Scans inside <b>.zip</b> , <b>.cab</b> , <b>.tar</b> , <b>.gz</b> , <b>.rar</b> , <b>.lzh</b> and <b>.arj</b> files.
-collect	Scans a virus collection.
-delete	Deletes infected files.
-disinf	Disinfects when possible. Deletes first-generation samples and files destroyed by overwriting viruses. It will never delete a file that can be disinfected.
-dumb	Scans all files. This switch is to be used with the <b>-collect</b> switch.
-follow	Follows symbolic links.
-help	Displays this list of switches.
-list	Lists all files being scanned.
-nobreak	Does not abort the scan if the <b>Ctrl-C</b> key combination is pressed.
-noheur	Disables heuristic scanning abilities.
-nosub	Does not scan subdirectories.
-notify=user@domain.com	When a virus is detected, sends an e-mail to the designated address (replace <b>user@domain.com</b> with a legitimate e-mail address).
-packed	Unpacks compressed executables.

Table 4: CSAV for FreeBSD Command-line Switches

Switch	Description
-quarantine=<directory name>	Quarantines the infected files to the directory specified at the command line. <b>Important:</b> Only users with root permissions can use this command-line option.
-rename	Renames infected <b>com/exe</b> files to <b>vom/vxe</b> .
-report=	Sends the output to a specified file.
-removeall	Removes all macros from all documents.
-removenew	Removes new variants of macro viruses by removing all macros from infected documents.
-saferemove	Removes all macros from all documents if a known virus is detected.
-silent	Does not generate any screen output.
-syslog	Logs all detected infections into the system log (usually /var/log/messages). <b>Important:</b> Only the root is allowed to use this switch as it generates additional output to the system files.
-virlist	If specified, displays the virus list on the screen. If used, this switch <b>must</b> be the <b>only</b> option. Use redirection to save the virus list as a file. For example: <pre>csav -virlist &gt; virlist.lis</pre> To view the virus list one screen at a time, you can use the <b> more</b> command: <pre>csav -virlist  more</pre>
-virno	Counts the known viruses.
	The following switches are non-functional in Command AntiVirus for FreeBSD: <b>-hard, -inter, -noboot, -nofile, -nofloppy, -nomem, -page, and -wrap.</b>

## E-mail Notification

Command AntiVirus for FreeBSD can be configured to send a virus notification e-mail message to a specific address. For example, when a virus is detected, an e-mail notification containing important information about the infection can be sent to a company's MIS department.

To enable e-mail notification, you must use the **-notify=user@domain.com** command-line switch (see **Table 4** located previously in this chapter). The default notification message is located in the **email.cfg** file. The default message is:

```
Dear Sir/Madam,  
  
On %DATE% Command AntiVirus version %VER% found the virus  
%VIRUS% in the file %FILE% (owned by %OWNER%) residing on  
the machine %MACHINE%.  
  
Regards,  
  
The Administrator
```



**NOTE:** You can use any standard text editor to reword the notification message to fit your needs.

When the notification message is generated, variables in **email.cfg** are replaced automatically with specific information about those variables. For example, if the **%VIRUS%** variable is used in **email.cfg**, the notification message will contain the name of the virus. A notification generated from the default **email.cfg** will look similar to the following:

```
Dear Sir/Madam,  
  
On Tue Aug 10 16:03:28 1999 Command AntiVirus version  
4.60.0 found the virus W97M/Test Macro in the file  
1/macro97.doc (owned by DBanner) residing on the  
machine hulk017.zigysoft.com.  
  
Regards,  
  
The Administrator
```

The variables that are available for use in the Command Antivirus virus notification e-mail message are described in the following table:

**Table 5: Notification Message Variables**

Variable	Description
%DATE%	Will be replaced with the current date. This variable reports the current day of the week, the calendar date, and the time of day.
%FILE%	Will be replaced with the name of the infected file.
%MACHINE%	Will be replaced with the machine name as found through DNS.
%OWNER%	Will be replaced by the user name of the owner of the infected file. <b>Important:</b> The owner is the account that currently “owns” the file. It is <b>not</b> guaranteed that this account created the file.
%VER%	Will be replaced with the version number of the currently running Command AntiVirus.
%VIRUS%	Will be replaced with the name of the virus infecting the file.

## REMOVING COMMAND ANTIVIRUS

---

To remove Command AntiVirus for FreeBSD, follow these steps:

1. At the FreeBSD command prompt, **\$**, type the following, and press **Enter**:

```
su
```

The system displays the **Password:** prompt.

2. Type your root password and press **Enter**.
3. To remove the deffiles package, at the command prompt, **#**, type the following and press **Enter**:

```
pkg_delete deffiles
```

4. To remove the Command AntiVirus package, at the command prompt, type the following and press **Enter**:

```
pkg_delete csav
```

5. To remove the documentation package, at the command prompt, type the following and press **Enter**:

```
pkg_delete csav-docs
```

6. To complete the removal of Command AntiVirus for FreeBSD, at the command prompt, type the following and press **Enter**:

```
exit
```

The system returns to the FreeBSD command prompt, **\$**.

