# Command AntiVirus™ for Linux

## 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.**


**Document No. CL-460-1200**

**Part No. PS 1126-10UG**

# TABLE OF CONTENTS

# INTRODUCTION

Command AntiVirus (CSAV) for Linux is a command-line scanner for the Linux operating system. It 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. CSAV now offers unparalleled protection and elimination of polymorphic viruses including the dreaded Morphine, Anxiety and Spanska.
- 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 the 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 PKZIP-compressed files and compressed executables including PKLite, DIET, ICE-PACK, WWPacked, ZIP, ARJ, RAR, CAB, TAR, LZH, and GZ.
- Can be configured to perform scheduled scans when used with the Linux cron utility.

# CHAPTER OVERVIEW

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

## Chapter 1 - Introduction

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

## Chapter 2 - Installation

Chapter 2 covers the product's installation and uninstall procedures.

## Chapter 3 - Using Command AntiVirus

This chapter provides information on how to perform virus scans and how to use the product's command line switches. Instructions are also for provided for using the CSAV for Linux e-mail notification feature.

## Chapter 4 - 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:

```
CSAV -HARD -DISINF
```

**CSAV** The acronym used for Command AntiVirus

# SYSTEM REQUIREMENTS

The system requirements for Command AntiVirus for Linux are:

- An IBM-compatible computer with a 386 or higher CPU
- Any version of Red Hat Linux Version 6.0 or higher, or SuSE Linux 6.2 or higher that is using the 2.0 kernel or higher.
- At least 3.0 MB of available hard disk space.
- GLIBC_2.0 or GLIBC_2.1 "C" runtime library.

# 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 **www.commandcom.com** or our web site in the United Kingdom at **www.command.co.uk**.

## HELP FILES

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

## MAILING LIST SERVER

Registered users of Command AntiVirus can subscribe to Command Software Systems' mailing list server. As long as you have an Internet e-mail address, you can obtain electronic notification of product updates and announcements. You

can also receive our newsletter, and a variety of other services. For more information, call Customer Satisfaction or visit our web site.

## README.TXT

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

# INSTALLATION

Installing Command AntiVirus for Linux is a straightforward process. 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.

## INSTALLING

We provide one installation package for Command AntiVirus for Linux: a shared package. Before starting this installation, be sure to determine whether your system is using **glibc2**.

To install Command AntiVirus for Linux, follow these instructions:

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. At the command prompt, type the following and press ENTER:

   # mount /mnt/cdrom

4. Type the following at the command prompt and press ENTER:

   # rpm -i /mnt/cdrom/csav-linux/i386/csav-4.60.0-shared.i386.rpm

5. At the command prompt, type the following and press ENTER:

```
# exit
```

This completes the installation of Command AntiVirus for Linux.

If you want to verify that Command AntiVirus is installed, type the following and press ENTER:

```
$ rpm -q csav
```

Your system should then display a “csav-x.xx.x-shared” message. The “x.xx.x” will be replaced by the Command AntiVirus version number thus confirming the installation.

## LOCATION OF INSTALLED FILES

For updating or troubleshooting purposes, you may need to know the location of the CSAV files that were installed on your system. For instance, you may need to know the locations of the **macro.def**, **sign2.def**, and **sign.def** files in order to update them occasionally. Table 1 provides the locations for the shared and static package files.

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

| Path | Description |
|---|---|
| /usr/bin/csav | The Command AntiVirus command line scanner. |
| /usr/lib/libcsscan.so | A symbolic link to the most recently installed shared library. |
| /usr/lib/libcsscan.so.x.xx | The shared library for CSAV. The “x.xx.x” will be replaced by the version number of the product. For instance, “4.60.0”. Note that **/usr/lib/libcsscan.so** (mentioned above) links to this specific file. |
| /etc/csav/english.tx1 | The file containing language-specific text. |
| /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. |
| /etc/csav/email.cfg | A sample e-mail notification file. This file can be used when -notify=user@domain is provided. Note that administrators can use a text editor to change the content of **email.cfg** to fit their needs. |
| /usr/doc/csav/distrib.txt | 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 often contains very important last-minute information about the functioning of the product. |
| /usr/doc/csav/legal.txt | Legal information regarding product copyright, licensing, usage, etc. |
| /usr/doc/csav/csslinux.pdf | The Command AntiVirus for Linux User’s Guide in pdf form. |
| /usr/doc/csav/guide.txt | The CSAV for Linux User’s Guide 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.

# TO REMOVE

If you want to remove Command AntiVirus for Linux, follow these instructions:

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. At the command prompt, type the following and press ENTER:

   ```
   # rpm -e csav
   ```

4. At the command prompt, type the following and press ENTER:

   ```
   # exit
   ```

You can then return to computing as normal.

# USING COMMAND ANTIVIRUS

Command AntiVirus for Linux is a powerful and easy-to-use command-line-based defense against computer viruses.

## PERFORMING A VIRUS SCAN

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

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

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

Note that you can scan more than one directory at a time. In the above example, 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 CSAV 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 above syntax:

“csav” is the Command AntiVirus executable

"{command line options}" can be any of the switches listed in this chapter's Table 1.

"path +" is one or more paths

For example, to scan all files in a directory called "doc", you could 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** performs a scan of the Master Boot Records (MBRs) and boot sectors of your local hard drives. It then displays the results of the scan.

**Table 2: CSAV for Linux Command Line Switches**

| Switch | Description |
|---|---|
| -all | Scans all files, when combined with another switch. |
| -append | Adds to the existing report file. This switch allows you to receive an extended report of what was scanned. If you use the **-list** command, this report could become very large so you will need to clear it frequently. The **-append** switch must be used with the **-report** switch. |
| -archive | Scans inside **.zip**, **.cab, .tar, .gz, .rar, .lzh** and **.arj** files. |

**Table 2: CSAV for Linux Command Line Switches**

| Switch | Description |
|---|---|
| -collect | Scan a virus collection. |
| -delete | Delete 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 | Do a “dumb” scan of all files. |
| -help | Display this list of switches. |
| -list | List all files being scanned. |
| -nobreak | Do not abort the scan if the CTRL-C key combination is pressed. |
| -noheur | Disable heuristic scanning abilities. |
| -nosub | Do not scan subdirectories. |
| -notify=user@domain.com | When a virus is detected, send an e-mail to the designated address (replace “user@domain.com” with a legitimate e-mail address). |
| -packed | Unpack compressed executables. |
| -rename | Rename infected **com/exe** files to **vom/vxe**. |
| -report= | Send the output to a specified file. |
| -removeall | Removes all macros from all documents. |
| -removenew | Remove new variants of macro viruses by removing all macros from infected documents. |
| -saferemove | Remove all macros from all documents if a known virus is detected. |
| -silent | Do not generate any screen output. |

**Table 2: CSAV for Linux Command Line Switches**

| Switch | Description |
|---|---|
| -syslog | Log all detected infections into the system log (usually /var/log/messages). IMPORTANT: Only the root is allowed to use this switch as it generates additional output to the system files. |
| -virlist | If specified, the virus list is displayed on-screen. If used, this switch must be the only option. Use redirection to save the virus list as a file. For example:<br><br>csav -virlist > virlist.lis<br><br>To view the virus list one screen at a time, you can use the **\|more** command:<br><br>csav -virlist \|more |
| -virno | Counts the known viruses. |

The following switches are non-functional in CSAV for Linux: **-hard**, **-inter**, **-noboot**, **-nofile**, **-nofloppy**, **-nomem**, **-page**, and **-wrap**.

## E-mail Notification

Command AntiVirus for Linux can be configured to send a virus notification e-mail message to a specific address. For instance, 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 the previous table). 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
```

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. Thus, a notification generated from the default **email.cfg** would 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 CSAV's virus notification e-mail message are described in the following table:

**Table 3: 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. IMPORTANT: The owner is the account that currently "owns" the file. It is **not** 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. |

# GLOSSARY

## BOOT SECTOR

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

## BOOT SECTOR VIRUS

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

## CIRCULAR INFECTION

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

## CMOS

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

## COMPANION VIRUS

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

## CROSS-LINKED FILES

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

## DROPPER

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

## EICAR TEST FILE

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

## ENCRYPTION

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

## EXECUTABLE CODE

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

## FALSE POSITIVE

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

## FILE STEALTH

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

## FULL STEALTH

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

## HEURISTICS

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

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

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

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

## INTEGRITY CHECKER

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

## JOKE PROGRAMS

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

## LOGIC BOMB

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

## MALWARE

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

## MACRO VIRUS

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

## MASTER BOOT RECORD (MBR)

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

## MEMORY-RESIDENT

Residing in computer memory as opposed to on the disk.

## MULTIPARTITE

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

## ON-ACCESS SCAN

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

## ON-DEMAND SCAN

A virus scan that is started manually. In 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.