

# Cleanscape Automated Source Analysis Fortran Installation Guide

Version 1.0



13170-B Central Ave. SE, STE 353  
Albuquerque, NM 87123  
Toll-free 800-94-4LINT  
[www.cleanscape.net](http://www.cleanscape.net)  
[sales@cleanscape.net](mailto:sales@cleanscape.net)  
[support@cleanscape.net](mailto:support@cleanscape.net)

**Note: Licensed users may photocopy for distribution.**

**Direct comments concerning this manual to the address on the title page or  
[support@cleanscape.net](mailto:support@cleanscape.net)**

**Copyright © 2017**

**CLEANSCAPE  
NOTICE OF COPYRIGHTS**

Copyrighted by Cleanscape as an unpublished work. All rights reserved. In claiming any copyright protection which may be applicable, Cleanscape reserves and does not waive any other rights that it may have (by agreement, statutory or common law, or otherwise) with respect to this material. See Notice of Proprietary Rights.

**NOTICE OF PROPRIETARY RIGHTS**

This manual and the material on which it is recorded are the property of Cleanscape. Its use, reproduction, transfer and/or disclosure to others, in this or any other form, is prohibited except as permitted by a written License Agreement with Cleanscape. Cleanscape reserves the right to update this document without prior notification.

Fortran-lint and CASAF are a trademarks of Cleanscape Software International.  
All other trademarks and registered trademarks are the property of their respective owners.

PART I	Introduction .....	1
1.1	WELCOME.....	1
1.2	DOCUMENTATION.....	1
1.3	PURPOSE.....	1
A.	Function .....	1
B.	Application.....	1
C.	Advantages .....	2
PART II	Requirements, Installation, and Uninstallation .....	3
2.1	WINDOWS.....	3
A.	System Requirements .....	3
B.	Software Setup Procedure.....	3
C.	Uninstallation – manual process.....	3
2.2	UNIX/LINUX .....	4
A.	System Requirements .....	4
B.	Software Setup Procedure.....	4
C.	Uninstallation – manual process.....	4
2.3	VMS .....	5
PART III	Activating CASAF.....	7
PART IV	Post-Installation Verification Test .....	9
APPENDIX A	ADDITIONAL STEPS FOR WINDOWS HOSTS .....	10
A.	Important note .....	10
B.	Details .....	10



## PART I Introduction

### 1.1 WELCOME

Thank you for your product purchase! Cleanscape Automated Source Analysis (CASA) is a family of tools that provide thorough and powerful static analysis of Common Weakness Enumeration (CWE) vulnerabilities in your source code.

CASAF is the designation of version that supports Fortran source. The acronym CASAF will be used throughout this Installation Guide.

### 1.2 DOCUMENTATION

CASA is at its core a command-line program. This Installation Guide provides installation and setup instructions, along with a command to validate the program post-installation.

Future releases may include other user interface modes; for assistance with these products, consult the relevant .pdf file located in your 'doc' subdirectory.

Your CASAF purchase also includes a full version of Cleanscape's venerable Fortran-lint (Flint) static analyzer. Please refer to flintman.pdf and flintgui.pdf located in the 'doc' subdirectory for usage details. It will be installed automatically during this process for CASAF.

### 1.3 PURPOSE

#### A. Function

CASAF is a CWE threat detector for Fortran source code. In version 1.0, CASAF's function is to detect the Top 25 weaknesses as enumerated in "2011 CWE/ SANS Top 25 Most Dangerous Software Errors" located at <http://cwe.mitre.org/top25/index.html>.

CASAF itself is hardened against cyber breaches. It self-repairs attempts to remove analyses or analysis results, and can report such attempts in a clandestine fashion to management (i.e., user is unaware her/his breach attempt was detected/ reported).

Future releases will increase the number of vulnerabilities detected, continually improve individual analysis capability, improve performance, and enhance resistance/ reporting mechanisms to tampering.

#### B. Application

Until recently, Fortran code was "grandfathered" from being subjected to vulnerability analysis because

- (a) it was commonly held that Fortran code was inherently safe (e.g., because no one writes a login routine or a web server in Fortran) and/or
- (b) something along the lines of, "Well, my Fortran code has been running for 30/40/50 years without incident, so it is de facto safe".

However, CWE vulnerability analysis of Fortran source code has recently become a requirement for many US government contracts. Furthermore, as we at Cleanscape assessed the Top 25 CWEs using real-world code, we found that neither of the above assumptions can be made – for instance, we found code on the web which validated SQL logins and even an entire web server written in Fortran – both of which contained CWE vulnerabilities!

Finally, since cyber attacks are already occurring in industries that commonly use Fortran, and attackers are constantly improving their tools and techniques, the prudent course is proactive prevention. Examples of attacks in industries that commonly use Fortran, such as aerospace, defense, energy, and simulation (though not necessarily attacks against Fortran code itself – yet):

- “The US Air Force’s Updated E-3G Radar Planes Are Vulnerable to Hacks”, *Motherboard*, 3-Mar-17
- “Could Terrorists Hack an Airplane? The Government Just Did”, *Daily Beast*, 17-Nov-17
- “U.S. Grid in ‘Imminent Danger’ From Cyber-Attack, Study Says”, *Bloomberg*, 6-Jan-17
- “Nuclear power plants vulnerable to hacking attack in ‘nightmare scenario’, UN warns”, *Independent UK*, 16-Dec-16
- “Chinese hack U.S. weather systems, satellite network”, *The Washington Post*, 12-Nov-14

### C. Advantages

1. The first (and as of version 1.0, *only*) CWE vulnerability analyzer for Fortran.
2. CWE threats are carefully reviewed and the concepts they describe have been thoroughly interpreted to extend their relevance to Fortran.
3. Detected threats are color coded using Homeland Security's Advisory System: Severe = **red**, High = **orange**, Elevated = **yellow**, and Guarded = **blue**.
4. The command line version is easy to operate, and output results are organized by test and colored according to the above Advisory scheme.
5. Built-in safeguards to prevent tampering and report such attempts to management without alerting the user.

## PART II Requirements, Installation, and Uninstallation

### 2.1 WINDOWS

#### A. System Requirements

##### 1. Hardware

Any configuration sufficient to run Windows is sufficient for the gr8utils.

##### 2. Operating System

Windows 7, Windows 8, Windows 10.

#### B. Software Setup Procedure

Please read the [\(Shrinkwrap\) Software License Agreement](#) first

##### 1. Installation

- a) Copy `casaf<ver>_win.exe` to a temporary directory, then run it.
- b) An installer window should appear. Click the OK button. This should extract a number of files to the directory you specified. The installer exits automatically, and no reboot is required.
- c) The installer adds the installation subdirectory to your system PATH – necessary for running CASAF (or any of the associated support programs) from the command line. To do this manually, run:  

```
set FLINTHOME=<install_dir>/flint/main;%PATH%  
set PATH=%FLINTHOME%;%PATH%
```
- d) Follow the instructions to obtain a license key as described in [Part 3](#).

##### 2. Additional steps for Windows access control

We recommend you install as Administrator. To make the program accessible to ordinary “Users”, some additional steps are required. For more information, see Appendix A.

#### C. Uninstallation – manual process

- a) Delete the installation directory and its subdirectories.
- b) Delete the installation directory from your PATH:  
Right click your “My Computer” icon on the desktop, select “Properties”, click the “Advanced” tab, click the “Environment Variables”, double-click the text field “Path” in the System Variables area, and from that string, delete the installation directory.

You can also use System Restore. The installer will create a Windows system restore point just prior to installation. If you have not added new programs in the interim, you can safely roll your system back to this point.

## 2.2 UNIX/LINUX

### A. System Requirements

#### 1. Hardware

A minimum of 2 GB memory is required for CASAF.

#### 2. Operating System.

- a. Most GNU/Linux OSes, including RedHat®, SuSE®, Debian®, Ubuntu®
- b. Mac OS-X® Tiger
- c. Sun Solaris®
- d. HP HP-UX® (PA-RISC and Itanium)
- e. SGI Irix®
- f. IBM AIX®

### B. Software Setup Procedure

Please read the ([Shrinkwrap](#)) [Software License Agreement](#) first

**Installation** – installation as root is easier and recommended. The ‘#’ below represents the root prompt.

- a) Download the latest version of `casaf<ver>_<OS>.taz` to a temporary directory, e.g., `/tmp`.
- b) Create installation directory, e.g., `/usr/local/cleanscape`, and `cd` to it.
- c) Use the following commands to extract the files:  

```
# gunzip /tmp/casaf<ver>_<OS>.taz
# tar xvf /tmp/casaf<ver>_<OS>.tar
```
- d) Set the environment (bash example):  

```
# export CSIAPPPBASE=<install_dir>
# export FLINTHOME=$CSIAPPPBASE/flintgui.dir/main
# export PATH=$CSIAPPPBASE:$FLINTHOME:$PATH
```
- e) Add read/write/execute permissions to projects subdirectory:  

```
# chmod 777 $CSIAPPPBASE/flintgui.dir/projects
```
- f) Follow the instructions to obtain a license key as described in [Part 3](#).
- g) Replicate the environment variables in each user’s init script (e.g., `.bashrc`).

### C. Uninstallation – manual process

- a) Delete the installation directory and its subdirectories.
- b) Delete the installation directory from `PATH`

## **2.3 VMS**

**TBD**



## PART III Activating CASAF

For CASAF version 1.0, two keys are required. 30-day temporary keys have been supplied to you via email as part of your purchase. If you did not receive them, contact [sales@cleanscape.net](mailto:sales@cleanscape.net).

*For Windows:*

Detailed instructions TBD. A temporary key is already in the distribution which minimizes license manager setup.

*For Unix and Linux:*

1. As root on the license server, run the command, `casaf activate`

If asked for the number of license servers, just hit <ENTER> to use the default of 1. If you need more than one, contact [support@cleanscape.net](mailto:support@cleanscape.net).

Enter the temp key identified in the email as "CASAF".

2. As root on the license server, run the command, `flint activate`

If asked for the number of license servers, just hit <ENTER> to use the default of 1.

Enter the temp key identified in the email as "Flint".

3. A script called 'startup' will be created. Run this script to initialize the license daemon. After a 3-minute delay (which occurs only during daemon startup), CASAF (and Flint) will be ready to use.

To have CASAF and Flint available after the license server reboots, you need an init script. To do so, contact us or see the 2nd entry of the FAQ at <http://downloads.cleanscape.net/flint/unixfaq.html>

4. To obtain your permanent keys, repeat `casaf activate` and send the server code to us via phone at 800-944-5468 or email [support@cleanscape.net](mailto:support@cleanscape.net). We will send you two permanent keys, one for CASAF and one for Flint.

Repeat steps 1 and 2 above, this time with your permanent keys. Rerunning 'startup' is not required, nor do you have to reboot the server or restart the daemon.

*For VMS:*

Detailed instructions TBD. Cleanscape plans to use HP license PAKs.



## PART IV Post-Installation Verification Test

To conclude the installation, run the command,

```
casaf -INSTALL_VERIFY
```

which will establish the health of your CASAF installation.

You can add the `-v` (verbose) option for more detailed output.

This option can be run periodically, if desired, to assess the status of your CASAF installation on a regular basis.

If you do not get an onscreen message indicating success, along with a nonzero exit code, refer to the messages for possible corrective actions or contact [support@cleanscape.net](mailto:support@cleanscape.net).

However, if successful, the following message will be output to the screen:

```
CASAF is healthy and ready to run.
```

and an exit code of 0 (zero) will be returned. In such instance, congratulations – CASAF installed properly and is ready for use!

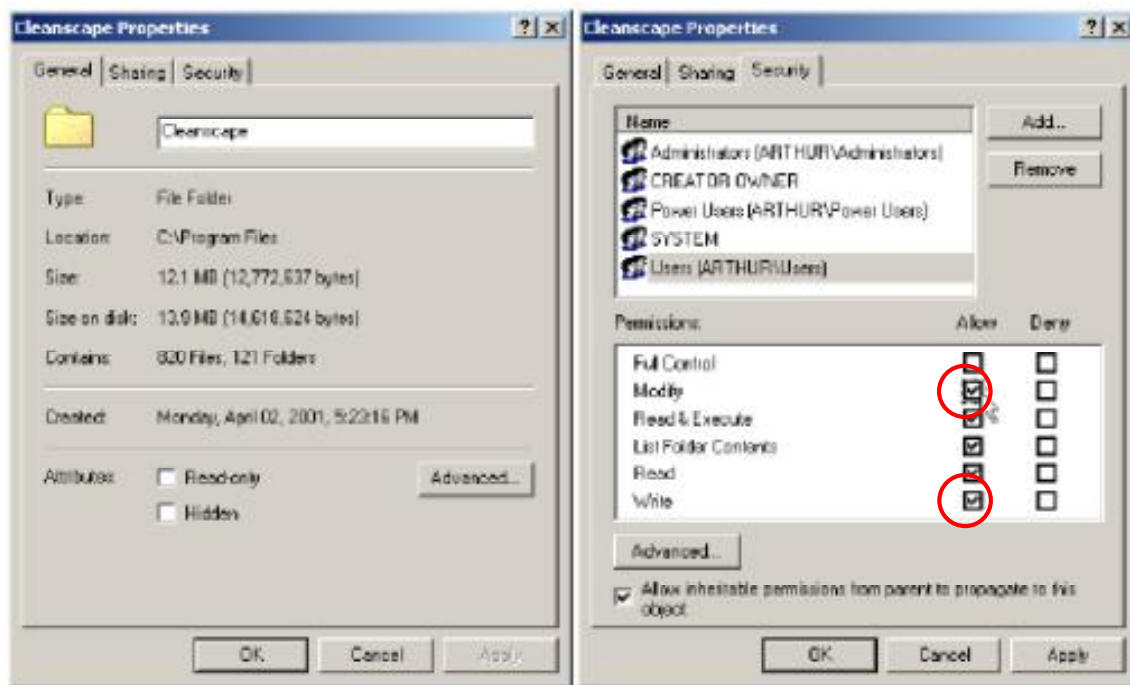
## APPENDIX A ADDITIONAL STEPS FOR WINDOWS HOSTS

### A. Important note

1. This section applies to users running Windows 2000, XP, Vista, 7, 8, and 10 who belong to the “Users” group, and only to that group.

### B. Details

1. For the product to run correctly under Win2k+, users must have “write” and “modify” access rights to the installation directory and all its subdirectories. This section explains the procedure used to change the access rights described above.
  - a. Log in as “administrator” and finish installing the product.
  - b. Double-click on the “My Computer” icon on the desktop.
  - c. Double-click installation folder. Select Properties from the sub-menu.
  - d. Select “Security” tab on the Properties screen (actual dialog may vary among Windows versions):



- e. Select the “Users” group and enable “Modify” and “Write” permissions.
- f. Click the “Apply” button.
- g. Click the “OK” button. This should close the Properties window.
- h. The product is now ready to run on Win2k for the “Users” group.