

# SOPHOS



## sophos anti-virus

### User manual

Sophos Anti-Virus for Linux, version 5

Document date: February 2006



## About this manual

This user manual explains how to use Sophos Anti-Virus for Linux and how to configure

- virus scanning
- virus alerts
- disinfection
- logging
- updating.

The manual also provides help in resolving common problems.

For information on the installation, initial setup or uninstallation of Sophos Anti-Virus, refer to the *Startup guide for Sophos Anti-Virus for Linux, version 5*.

Sophos documentation is published at [www.sophos.com/support/docs/](http://www.sophos.com/support/docs/) and on the Sophos CDs.

# Contents

Conventions used in this manual	5
<b>Using Sophos Anti-Virus</b>	
1 About Sophos Anti-Virus	8
2 Running on-access scanning	11
3 Running on-demand scans	14
4 What happens if a virus is found?	17
5 Cleaning up viruses	18
6 Viewing the logs	23
<b>Configuring Sophos Anti-Virus</b>	
7 Overview of configuration	26
8 Configuring on-access scanning	31
9 Configuring on-demand scanning	47
10 Configuring alerts	57
11 Configuring the Sophos Anti-Virus log	68
12 Configuring the Sophos Anti-Virus GUI	69
<b>Updating Sophos Anti-Virus</b>	
13 Updating Sophos Anti-Virus immediately	72
14 Kernel support	73
15 Configuring updating	74
<b>Troubleshooting</b>	
16 Troubleshooting	82

**Appendix**

Appendix 1 Locales 88

**Glossary and index**

Glossary 92

Index 95

Technical support 97

## Conventions used in this manual

Where command-line input continues over more than one line, subsequent lines are shown indented, for example

```
/opt/sophos-av/bin/savconfig -f corpconfig.cfg -c ScanOnEnable  
    mounted
```

You should type what is printed without inserting a line break.



# ***Using Sophos Anti-Virus***

**About Sophos Anti-Virus**

**Running on-access scanning**

**Running on-demand scans**

**What happens if a virus is found?**

**Cleaning up viruses**

**Viewing the logs**

# 1 About Sophos Anti-Virus

## 1.1 User interfaces

Sophos Anti-Virus can be used in two ways:

- via the command line
- via the Sophos Anti-Virus graphical user interface (GUI).

The command line enables you to access *all* the Sophos Anti-Virus functionality and to perform *all* configuration. The command line is the only way to use and configure on-demand scanning and updating.

- 💡 This manual assumes that you have installed Sophos Anti-Virus in the default location. Therefore, the paths of the commands described are based on this location.

The Sophos Anti-Virus GUI enables you to

- check the status of on-access scanning
- start and stop on-access scanning
- configure on-access scanning
- configure alerts
- view the Sophos Anti-Virus log
- configure cleanup.

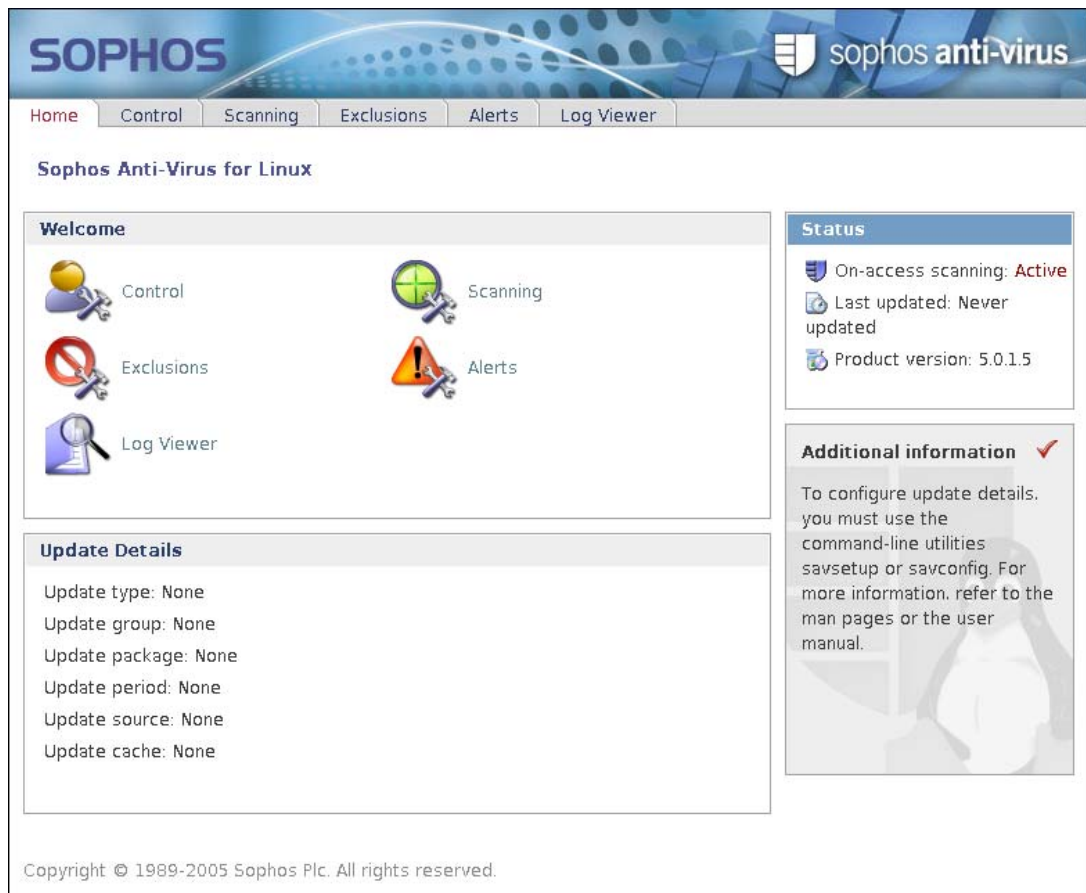
- ⚠ Although the GUI can be run by the root user (as well as other users), it doesn't run with root privileges. Therefore, it can't access all files on the computer.

To use the GUI, open a browser. In the address text box, type

`http://localhost:8081`

- 💡 If you want to use a different http port in the address, configure the GUI as explained in [section 12](#).

The browser displays the home page of the GUI.



When you browse to another page, the browser asks you for your credentials.

To find out your username, either ask your system administrator or, at the command line, type

```
/opt/sophos-av/bin/savconfig query HttpUsername
```

To find out your password, either ask your system administrator or, at the command line, type

```
/opt/sophos-av/bin/savconfig query HttpPassword
```

To change your credentials, refer to [section 12](#).

## 1.2 Scanning modes

Sophos Anti-Virus has two modes of scanning:

- on-access
- on-demand.

**On-access scanning** intercepts files as they are accessed, and grants access to only those that are virus free.

An **on-demand scan** is a virus scan of the computer, or parts of the computer, that you can run immediately or schedule to run at another time.

## 2 Running on-access scanning

- ❓ **On-access scanning** intercepts files as they are accessed, and grants access to only those that are virus free.

This section tells you how to *use* on-access scanning. To *configure* it, refer to [section 8](#).

### 2.1 Checking on-access scanning is active

#### Command line

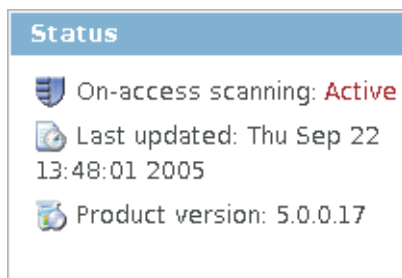
If you have root privileges, type

```
/opt/sophos-av/bin/savdstatus
```

Sophos Anti-Virus displays the status of on-access scanning.

#### GUI

On each page, in the **Status** panel, the status of on-access scanning is displayed.



### 2.2 Checking on-access scanning will be started automatically on system boot

#### Command line

Type

```
chkconfig --list
```

- ❗ This command might not work on TurboLinux.

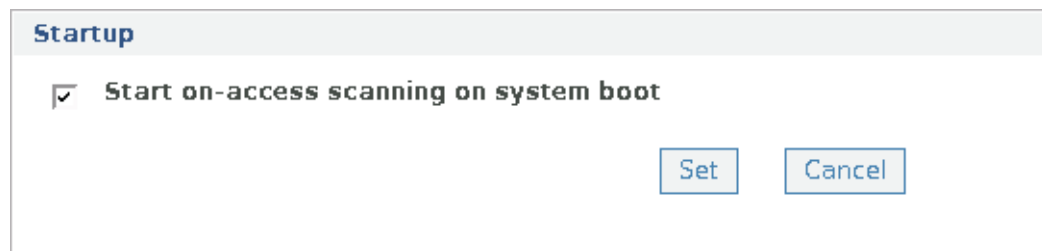
If the list contains an entry for sav-protect with 2:on, 3:on, 4:on and 5:on, on-access scanning will be started automatically on system boot.

Otherwise, to start on-access scanning automatically on system boot, type

```
/opt/sophos-av/bin/savdctl enableOnBoot savd
```

## GUI

On the **Control** page, in the **Startup** panel, see if the check box labeled **Start on-access scanning on system boot** is selected. If it is not, select it to start on-access scanning automatically on system boot. Click **Set** to apply the change.



## 2.3 Starting on-access scanning

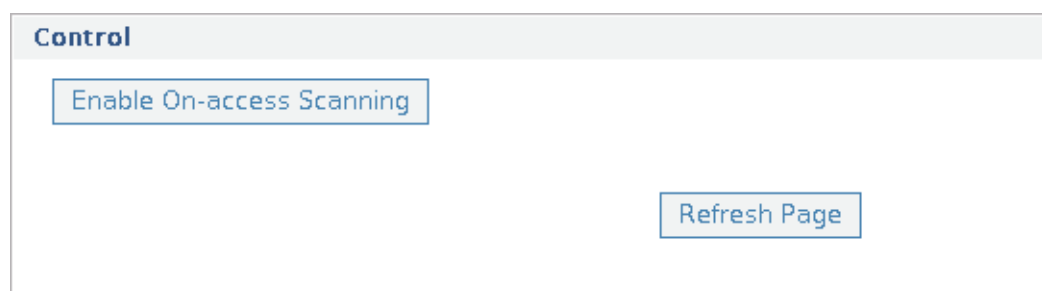
### Command line

Type

```
/etc/init.d/sav-protect start
```

### GUI

On the **Control** page, in the **Control** panel, click **Enable On-access Scanning**.



## 2.4 Stopping on-access scanning

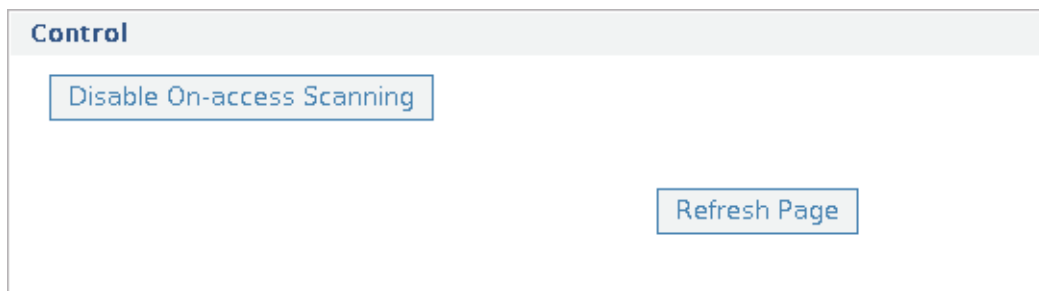
### Command line

Type

```
/etc/init.d/sav-protect stop
```

### GUI

On the **Control** page, in the **Control** panel, click **Disable On-access Scanning**.



## 3 Running on-demand scans

- ❓ An **on-demand scan** is a virus scan of the computer, or parts of the computer, that you can run immediately or schedule to run at another time.

By default, Sophos Anti-Virus scans

- executable Windows files
- .sh and .pl files
- files that can contain macros
- HTML files
- files compressed with PKLite, LZEXE and Diet
- directories below the one specified
- items pointed to by symbolic links.

For a full list of the file types scanned, type

```
savscan -vv
```

For information on changing these settings, see [section 9](#).

- 💡 Sophos Anti-Virus can scan Linux computers at set times automatically. This is done using the crontab facility. See the documentation for your computer.

### 3.1 Scanning the computer

To scan the computer, type

```
savscan /
```

### 3.2 Scanning a particular directory or file

To scan a particular directory or file, use the path of the item to be scanned, for example

```
savscan /usr/mydirectory/myfile
```

### 3.3 Scanning a filesystem

To scan a filesystem, use the name of the filesystem, for example

```
savscan /home
```

More than one filesystem can be entered at the command line.

### 3.4 Scanning a boot sector

You can scan boot sectors of logical and physical drives.

To scan boot sectors, log in as superuser (to get sufficient permission to access the disk devices) and then use one of the commands shown below.

To scan the boot sectors of specified logical drives, type

```
savscan -bs=XXX, XXX, ...
```

where XXX is the name of a drive (for example /dev/fd0 or /dev/hda1).

To scan boot sectors for all logical drives that Sophos Anti-Virus recognises, type

```
savscan -bs
```

To scan the master boot records for all the fixed physical drives on the computer, type

```
savscan -mbr
```

### 3.5 Scheduling a scan

To scan the computer at set times automatically, use the crontab facility. Refer to your Linux documentation.

### 3.6 Error codes

Sophos Anti-Virus returns error codes if there is an error or if a virus is found.

- 0 If no errors are encountered and no viruses are found.
- 1 If the user interrupts the execution by pressing 'Ctrl'+ 'c'.
- 2 If some error preventing further execution of a scan is discovered.
- 3 If viruses or virus fragments are discovered.

### **3.6.1 Extended error codes**

A different set of error codes are returned if the savscan command is run with the -eec qualifier.

- 0 If no errors are encountered and no viruses are found.
- 8 If survivable errors have occurred.
- 16 If password-protected files have been found. (They are not scanned.)
- 20 If viruses have been found and disinfected.
- 24 If viruses have been found and not disinfected.
- 28 If viruses have been found in memory.
- 32 If there has been an integrity check failure.
- 36 If unsurvivable errors have occurred.
- 40 If execution has been interrupted.

## 4 What happens if a virus is found?

### 4.1 If a virus is found during on-access scanning

If Sophos Anti-Virus finds a virus during an on-access scan, it denies access to the file and displays a message box like the one shown below.

If the message box cannot be displayed, the alert is shown at the command line.

Refer to [section 5](#) for information on cleaning up viruses.



### 4.2 If a virus is found when you run an on-demand scan

If Sophos Anti-Virus finds a virus, it reports it on the line which starts with >>> followed by either “Virus” or “Virus Fragment”:

```
SAVScan virus detection utility
Version X.XX.XX, May 2005 [Linux/Intel]
Virus data version X.XX, May 2005
Includes detection for 103269 viruses, trojans and worms
Copyright (c) 1989,2005 Sophos Plc, www.sophos.com

System time 10:23:49, System date 10 May 2005

Quick Scanning

>>> Virus 'EICAR-AV-Test' found in file /usr/mydirectory/eicar.src

33 files swept in 2 seconds.
1 virus was discovered.
1 file out of 33 was infected.
Please send infected samples to Sophos for analysis.
For advice consult www.sophos.com, email support@sophos.com
or telephone +44 1235 559933
End of Scan.
```

Refer to [section 5](#) for information on cleaning up viruses.

## 5 Cleaning up viruses

### 5.1 Getting cleanup information

If a virus is reported, you can get information and cleanup advice from the Sophos website. Go to the virus analyses page ([www.sophos.com/virusinfo/analyses](http://www.sophos.com/virusinfo/analyses)). Search for the analysis of the virus, by using the name that was reported by Sophos Anti-Virus.

### 5.2 Setting up automatic cleanup for on-access scanning

Sophos Anti-Virus can disinfect or delete infected items automatically, when on-access scanning is running. Any actions that Sophos Anti-Virus takes against infected items are logged in the Sophos Anti-Virus log. By default, automatic cleanup is disabled.

#### Command line

To enable automatic deletion of infected files, type

```
/opt/sophos-av/bin/savconfig AutomaticAction delete
```

- ❗ You should use this option only if advised to by Sophos technical support. If the infected file is a mailbox, Sophos Anti-Virus might delete the whole mailbox.

To disable automatic deletion, type

```
/opt/sophos-av/bin/savconfig remove AutomaticAction delete
```

To enable automatic disinfection of infected files and boot sectors, type

```
/opt/sophos-av/bin/savconfig AutomaticAction disinfect
```

Disinfection of documents does not repair any changes the virus has made in the document. (Refer to section 5.1 to find out how to view details on the Sophos website of the virus's side-effects.) Disinfection of programs should be used only as a temporary measure. You should subsequently replace disinfected programs from the original disks or a clean backup.

To disable automatic disinfection, type

```
/opt/sophos-av/bin/savconfig remove AutomaticAction disinfect
```

If you enable both automatic deletion and disinfection, Sophos Anti-Virus first tries to *disinfect* the item. If disinfection fails, it deletes it.

## GUI

To set up automatic cleanup, go to the **Scanning** page, **Cleanup** panel.

**Cleanup**

**Automatically disinfect infected items**

If you do not use automatic disinfection, or if disinfection fails, what do you want to do with infected items?

**Automatically delete infected items**

Set Cancel

Configure cleanup as described below. When you have done this, click **Set** to apply the changes. To undo any changes that you have made since you last clicked **Set**, click **Cancel**.

To enable automatic deletion of infected files, select the **Automatically delete infected items** check box.

- ❗ You should use this option only if advised to by Sophos technical support. If the infected file is a mailbox, Sophos Anti-Virus might delete the whole mailbox.

To enable automatic disinfection of infected files and boot sectors, select the **Automatically disinfect infected items** check box. Disinfection of documents does not repair any changes the virus has made in the document. (Refer to [section 5.1](#) to find out how to view details on the Sophos website of the virus's side-effects.) Disinfection of programs should be used only as a temporary measure. You should subsequently replace disinfected programs from the original disks or a clean backup.

If you enable both automatic deletion and disinfection, Sophos Anti-Virus first tries to *disinfect* the item. If disinfection fails, it deletes it.

### 5.3 Setting up automatic cleanup for on-demand scanning

Sophos Anti-Virus can disinfect or delete infected items automatically, when you run an on-demand scan. Any actions that Sophos Anti-Virus takes against infected items are listed in the scan summary and logged in the Sophos Anti-Virus log. By default, automatic cleanup is disabled.

The method you use depends on whether you want to disinfect a data file, a program, or a boot sector.

### 5.3.1 Disinfecting a data file

To disinfect a specific data file (e.g. a document or spreadsheet), type

```
savscan DATA-FILE-PATH -di
```

Alternatively, to detect and remove viruses in any data file or program on the computer, type

```
savscan / -di
```

In either case, Sophos Anti-Virus asks for confirmation before it disinfects.

Disinfection of documents does not repair any changes the virus has made in the document. (Refer to [section 5.1](#) to find out how to view details on the Sophos website of the virus's side-effects.)

### 5.3.2 Cleaning up viruses in a Windows program

You can cleanup viruses in program files in two ways.

**To disinfect a program file**, type

```
savscan PROGRAM-FILENAME -di
```

This ensures that the virus cannot spread. However, the program file may be corrupted. You should subsequently delete it and replace it from a backup.

**To delete an infected program file**, type

```
savscan PROGRAM-FILENAME -remove
```

Alternatively, to delete all infected programs, type

```
savscan / -remove
```

In either case, Sophos Anti-Virus asks for confirmation before it deletes the program(s).

### 5.3.3 Disinfecting a boot sector

To disinfect a boot sector, type

```
savscan -bs=XXX -di
```

where **XXX** is the name of a drive.

For example, to eliminate a virus in the floppy drive, type

```
savscan -bs=/dev/fd0 -di
```

### 5.3.4 Quarantining infected files

You can configure Sophos Anti-Virus to put infected files into quarantine (i.e. to prevent them from being accessed). It does this by changing the ownership and permissions for the file.

To specify quarantining, type

```
savscan PATH --quarantine
```

where PATH is the path to be scanned.

By default, Sophos Anti-Virus changes the ownership of an infected file to that of the user running Sophos Anti-Virus and changes the file permissions to `-r-----` (0400).

If you prefer, you can specify the user or group ownership and file permissions that Sophos will apply to infected files. You do so by using the parameters

```
uid=NNN
user=USERNAME
gid=NNN
group=GROUP-NAME
mode=PPP
```

You cannot specify more than one parameter of each type, e.g. you cannot enter the same username twice, or enter a uid and a username.

For each parameter you do not specify, the default setting (as given above) is used.

For example:

```
savscan fred --quarantine:user=sophosav,group=virus,mode=0400
```

will change an infected file's user ownership to `sophosav`, the group ownership to `virus`, and the file permissions to `-r-----`. This means the file is owned by the user `sophosav` and group `virus`, but *only* the user `sophosav` can access the file (and only for reading). No one else can do anything to the file (apart from root).

- ❗ If you specify cleanup as well as quarantining, Sophos Anti-Virus attempts to cleanup infected items and quarantines them only if cleanup fails.

## 5.4 Recovering from virus side-effects

Recovery from virus infection depends on how the virus infected the computer. Some viruses leave you with no side-effects to deal with, others may have such extreme side-effects that you have to restore a hard disk in order to recover.

Some viruses gradually make minor changes to data. This type of corruption can be hard to detect. It is therefore very important that you read the virus analysis on the Sophos website, and check documents carefully after disinfection.

Sound backups are crucial. You should keep original executables on write-protected disks so that infected programs can easily be replaced. If you did not have them before you were infected, create or obtain them in case of future infections.

Sometimes you can recover data from disks damaged by a virus. Sophos can supply utilities for repairing the damage caused by some viruses. Contact Sophos [technical support](#) for advice.

## 6 Viewing the logs

Sophos Anti-Virus logs details of scanning activity in the Sophos Anti-Virus log and syslog. In addition, virus and error events are logged in the Sophos Anti-Virus log. Messages in the Sophos Anti-Virus log are translated into the languages that the product supports.

### Command line

Use the command `savlog`. This can be used with various command-line options to restrict the output to certain messages and control the display. For example, to display all messages logged to the Sophos Anti-Virus log in the last 24 hours, and to display the date and time in UTC/ISO 8601 format, type

```
/opt/sophos-av/bin/savlog --today --utc
```

To see a complete list of the options that can be used with `savlog`, type

```
man savlog
```

## GUI

Go to the **Log Viewer** page.

### Log Selection

**Display log entries after**

**Display log entries before**

**Maximum number of log entries**

**Category**

**Time format**

Local time

UTC

[View Log](#)

### Log Contents

Time	Category	Event
Mon 16 Jan 2006 15:44:04 GMT	savd.daemon	Sophos Anti-Virus daemon started.
Mon 16 Jan 2006 17:41:46 GMT	savd.daemon	On-access scanning enabled.
Mon 16 Jan 2006 19:09:46 GMT	savd.daemon	On-access scanning disabled.
Tue 17 Jan 2006 13:55:27 GMT	savd.daemon	On-access scanning enabled.
Tue 17 Jan 2006 13:57:29 GMT	savd.daemon	On-access scanning enabled.

Using the text boxes and radio buttons in the **Log Selection** panel, specify the messages that you want to display. Then click **View Log** to display the messages in the **Log Contents** panel.

# ***Configuring Sophos Anti-Virus***

**Overview of configuration**

**Configuring on-access scanning**

**Configuring on-demand scanning**

**Configuring alerts**

**Configuring the Sophos Anti-Virus log**

**Configuring the Sophos Anti-Virus GUI**

## 7 Overview of configuration

### 7.1 Using savconfig

savconfig is the command that you use to set or query configuration of Sophos Anti-Virus. The path of the command is /opt/sophos-av/bin.

The syntax of savconfig is

```
savconfig [OPTION] ... [OPERATION] [PARAMETER] [VALUE] ...
```

To view a complete list of the options, operations and parameters, type

```
man savconfig
```

However, the following is an overview.

#### 7.1.1 OPTION

You can specify one or more options. The options are mainly associated with the *layers* in the local configuration files in each installation. For information on layers, refer to [section 7.3.3](#). By default, the command accesses the User layer. Therefore, if you want to access the Corporate layer for example, use the option -c or --corporate.

By default, the values of parameters in the Corporate layer are locked, so that they override values in the User layer. However, if you want to allow a corporate setting to be overridden by users, use the option --nolock. For example, to set the value of LogMaxSizeMB and allow it to be overridden, type

```
/opt/sophos-av/bin/savconfig --nolock -f corpconfig.cfg -c  
LogMaxSizeMB 50
```

#### 7.1.2 OPERATION

You can specify one operation. The operations are mainly associated with how you want to access a parameter. Some parameters can have only one value but others can have a list of values. Therefore, the operations enable you to add values to a list or remove values from a list. For example, the CacheFilesystems parameter is a *list* of filesystem types.

#### 7.1.3 PARAMETER

You can specify one parameter. To list all the parameters that can be set, type

```
/opt/sophos-av/bin/savconfig -v
```

Some parameters require secondary parameters to be specified as well. For example, if you want to specify the message that gets emailed when there is a virus, you must specify the language as well (in this case English):

```
/opt/sophos-av/bin/savconfig ThreatMessage en 'Contact IT'
```

#### 7.1.4 VALUE

You can specify one or more values that will be assigned to a parameter. If a value contains spaces, you must enclose it in single quotes.

## 7.2 Using savsetup

savsetup is the utility that you use to set or query configuration of updating and the Sophos Anti-Virus GUI. Although it enables you to access only some of the parameters that you can access with savconfig, it is easier to use. To run savsetup, type

```
/opt/sophos-av/bin/savsetup
```

When you run savsetup, it gives you a choice of configuration: updating or the Sophos Anti-Virus GUI. Enter the appropriate number to make your choice. Continue by responding to the questions that are displayed.

## 7.3 Configuring Sophos Anti-Virus across a network

If you have installed Sophos Anti-Virus across a network, you can configure Sophos Anti-Virus on the whole or part of the network by creating and updating a corporate configuration file in the central installation of Sophos Anti-Virus. Then, when workstations update from the central installation, they use this configuration.

There are two corporate configuration files: the *live* corporate configuration file in the central installation directory (CID) and the *offline* corporate configuration file stored elsewhere. When you want to change the live file, you change the offline file, and use a program to replace the live file with the offline file.

### 7.3.1 Creating the live corporate configuration file in the CID

1. Create the offline corporate configuration file in a directory of your choice other than the CID. You must use the command `savconfig`, and specify
  - the name of the offline file, including a filename extension `cfg`
  - that you are accessing the *Corporate* layer of the file
  - the setting of a parameter.

Use the following syntax:

```
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c PARAMETER VALUE
```

where `CONFIG-FILE` is the path of the offline file, `PARAMETER` is the parameter that you want to set and `VALUE` is the value to which you want to set the parameter. For example, to create a file called `corpconfig.cfg` and to add all mounted drives to the list of items to scan when on-access scanning is started, type

```
/opt/sophos-av/bin/savconfig -f corpconfig.cfg -c ScanOnEnable  
mounted
```

For information on using `savconfig`, refer to [section 7.1](#).

2. Set other parameters, as necessary, using the command `savconfig`. You must specify the name of the offline file and that you are accessing the Corporate layer, as above.
3. To view the settings of parameters, use the query operation. You can view the setting of an individual parameter or all parameters. For example, to view the settings of all the parameters that you have set, type

```
/opt/sophos-av/bin/savconfig -f corpconfig.cfg -c query
```

4. When you have finished setting parameters, run the `addcfg` utility to copy the configuration to the central installation directory (CID), ready for workstations to download when they next update. The utility is in the CID. Depending on where the CID is, type

```
/opt/sophos-av/update/cache/LOCAL/PACKAGE/addcfg.sh -fCONFIG-FILE
```

where `CONFIG-FILE` is the path of the offline file.

### 7.3.2 Updating the live corporate configuration file in the CID

1. Update the offline corporate configuration file. You must use the command `savconfig`, and specify
  - the name of the offline file
  - that you are accessing the *Corporate* layer of the file
  - the setting of a parameter.

Use the following syntax:

```
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c PARAMETER VALUE
```

where `CONFIG-FILE` is the path of the offline file, `PARAMETER` is the parameter that you want to set and `VALUE` is the value to which you want to set the parameter. For example, to update a file called `corpconfig.cfg` and to add all mounted drives to the list of items to scan when on-access scanning is started, type

```
/opt/sophos-av/bin/savconfig -f corpconfig.cfg -c LogMaxSizeMB 50
```

For information on using `savconfig`, refer to [section 7.1](#).

2. Set other parameters, as necessary, using the command `savconfig`. You must specify the name of the offline file and that you are accessing the Corporate layer, as above.
3. To view the settings of parameters, use the query operation. You can view the setting of an individual parameter or all parameters. For example, to view the settings of all the parameters that you have set, type

```
/opt/sophos-av/bin/savconfig -f corpconfig.cfg -c query
```

4. When you have finished setting parameters, run the `addcfg` utility to copy the configuration to the central installation directory, ready for workstations to download when they next update. The utility is in the CID. Depending on where the CID is, type

```
/opt/sophos-av/update/cache/LOCAL/PACKAGE/addcfg.sh -fCONFIG-FILE
```

where `CONFIG-FILE` is the path of the offline file.

### 7.3.3 Configuration layers

Each installation of Sophos Anti-Virus includes a local configuration file, which includes settings for all parts of Sophos Anti-Virus.

Each local configuration file contains a number of *layers*:

- **Sophos:** This is always present in the file. It includes the factory settings, which are changed only by Sophos.
- **Corporate:** This is present if the installation is configured from the central installation directory (CID), as described in sections 7.3.1 and 7.3.2.
- **User:** This is present if any local configuration is performed. It includes settings that apply only to the installation on this computer.

Each layer uses the same parameters, so that the same parameter can be set in more than one layer. However, when Sophos Anti-Virus checks the value of a parameter, it does so according to the layer hierarchy:

- By default, Corporate layer overrides User layer.
- Corporate and User layers override Sophos layer.

For example, if a parameter is set in the User layer and the Corporate layer, the value in the Corporate layer is used. Nevertheless, you can unlock the values of individual parameters in the Corporate layer, so that they can be overridden.

When the local configuration file is updated from the corporate configuration file, the Corporate layer in the local file is replaced by that of the corporate file.

## 7.4 Configuring Sophos Anti-Virus on a single computer

Use the command `savconfig` to perform configuration on a single computer. For information on using `savconfig`, refer to [section 7.1](#). By default, `savconfig` applies configuration to the User layer of the local configuration file.

## 8 Configuring on-access scanning

- ❗ If you are configuring a single computer that is on a network, such configuration might be discarded if the computer downloads a new corporate configuration.

### 8.1 Configuring what is or is not scanned when on-access scanning is started or stopped

You can configure which devices have their boot sectors scanned and which devices do *not* have their boot sectors scanned when on-access scanning changes from being disabled to enabled or vice-versa.

In the following subsections, you must specify the path(s) of the device(s) to be scanned or one of the following values:

mounted	All mounted devices
bootable	All devices that can be booted from
hd	All hard disks
floppy	All floppy disks
cd	All CDs
dvd	All DVDs

#### 8.1.1 What is scanned when on-access scanning is started

To see the default list of devices that have their boot sectors scanned when on-access scanning is started, type

```
/opt/sophos-av/bin/savconfig -s query ScanOnEnable
```

To change the list of devices, use the ScanOnEnable parameter. You must specify the path(s) of the device(s) or one of the values listed above. For example, to add all devices that can be booted from to the list of devices, type

```
/opt/sophos-av/bin/savconfig ScanOnEnable bootable
```

To remove a device from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove ScanOnEnable bootable
```

### 8.1.2 What is not scanned when on-access scanning is started

To see the default list of devices that don't have their boot sectors scanned when on-access scanning is started, type

```
/opt/sophos-av/bin/savconfig -s query NoScanOnEnable
```

To change the list of devices, use the NoScanOnEnable parameter. You must specify the path(s) of the device(s) or one of the values listed above. For example, to add all CD drives to the list of devices, type

```
/opt/sophos-av/bin/savconfig NoScanOnEnable cd
```

To remove a device from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove NoScanOnEnable cd
```

### 8.1.3 What is scanned when on-access scanning is stopped

To see the default list of devices that have their boot sectors scanned when on-access scanning is stopped, type

```
/opt/sophos-av/bin/savconfig -s query ScanOnDisable
```

To change the list of devices, use the ScanOnDisable parameter. You must specify the path(s) of the device(s) or one of the values listed above. For example, to add all devices that can be booted from to the list of devices, type

```
/opt/sophos-av/bin/savconfig ScanOnDisable bootable
```

To remove a device from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove ScanOnDisable bootable
```

### 8.1.4 What is not scanned when on-access scanning is stopped

To see the default list of devices that don't have their boot sectors scanned when on-access scanning is stopped, type

```
/opt/sophos-av/bin/savconfig -s query NoScanOnDisable
```

To change the list of devices, use the NoScanOnDisable parameter. You must specify the path(s) of the device(s) or one of the values listed above. For example, to add all CD drives to the list of devices, type

```
/opt/sophos-av/bin/savconfig NoScanOnDisable cd
```

To remove a device from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove NoScanOnDisable cd
```

## 8.2 Allowing access to corrupt files that can't be scanned

- By default, Sophos Anti-Virus allows access to all types of corrupt file that can't be scanned. To allow access to only particular types of corrupt file, deny access to all types of corrupt file by typing

```
/opt/sophos-av/bin/savconfig DenyOnCorruptFile enabled
/opt/sophos-av/bin/savconfig DenyOnDetectionError enabled
```

and then allow access to particular file types as explained below.

### Command line

To allow access to files of a particular type that appear to Sophos Anti-Virus to be corrupt, use the `AllowIfCorrupt` parameter. To see the default list of file types, type

```
/opt/sophos-av/bin/savconfig -s query AllowIfCorrupt
```

To change the list of file types, specify either an asterisk `*` or a value that is returned by the `file` command. (For more information on the `file` command, type `man file`.) An asterisk means any file type. For example, to add XML files to the list of file types, type

```
/opt/sophos-av/bin/savconfig AllowIfCorrupt 'XML document text'
```

To remove a file type from the list, use the `remove` operation. For example, type

```
/opt/sophos-av/bin/savconfig remove AllowIfCorrupt 'XML document
text'
```

- Sophos Anti-Virus performs partial matching of file types. Thus, it excludes all file types that match the specified file type up to the number of characters in the specified file type, starting from the left. For example, 'TIFF' excludes all types of TIFF file, but 'TIFF image data, little-endian' excludes only certain types of TIFF file.

### GUI

To allow access to files of a particular type that appear to Sophos Anti-Virus to be corrupt, on the **Exclusion Configuration** page, in the **Error Exclusions** panel, type the file type in the text box labeled **File types to allow access to if the file is corrupt**. The file type must be either an asterisk `*` or a value that is returned by the `file` command. An asterisk means any file type. (For

more information on the file command, type `man file`.) Click **Add New Entry** to add the file type to the list.

**File types to allow access to if the file is corrupt**

TIFF image data. little-endian	<a href="#">Add New Entry</a>
XML document text	
<a href="#">Remove Selected Entry</a>	

To remove a file type from the list, select the file type and click **Remove Selected Entry**.

- 💡 Sophos Anti-Virus performs partial matching of file types. Thus, it excludes all file types that match the specified file type up to the number of characters in the specified file type, starting from the left. For example, 'TIFF' excludes all types of TIFF file, but 'TIFF image data, little-endian' excludes only certain types of TIFF file.

## 8.3 Allowing access to encrypted files that can't be scanned

### Command line

To allow access to files of a particular type that are encrypted, use the `AllowIfEncrypted` parameter. To see the default list of file types, type

```
/opt/sophos-av/bin/savconfig -s query AllowIfEncrypted
```

To change the list of file types, specify either an asterisk `*` or a value that is returned by the file command. (For more information on the file command, type `man file`.) An asterisk means any file type. For example, to add all file types to the list of file types, type

```
/opt/sophos-av/bin/savconfig AllowIfEncrypted '*'
```

To remove a file type from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove AllowIfEncrypted '*'
```

- 💡 Sophos Anti-Virus performs partial matching of file types. Thus, it excludes all file types that match the specified file type up to the number of characters in the specified file type, starting from the left. For example, 'TIFF' excludes all types of TIFF file, but 'TIFF image data, little-endian' excludes only certain types of TIFF file.

## GUI

To allow access to files of a particular type that are encrypted, on the **Exclusion Configuration** page, in the **Error Exclusions** panel, type the file type in the text box labeled **File types to allow access to if the file is encrypted**. The file type must be either an asterisk `*` or a value that is returned by the file command. An asterisk means any file type. (For more information on the file command, type `man file`.) Click **Add New Entry** to add the file type to the list.

**File types to allow access to if the file is encrypted**

ASCII English text	<a href="#">Add New Entry</a>
PDF document. version 1.3	
<a href="#">Remove Selected Entry</a>	

To remove a file type from the list, select the file type and click **Remove Selected Entry**.

- ❗ Sophos Anti-Virus performs partial matching of file types. Thus, it excludes all file types that match the specified file type up to the number of characters in the specified file type, starting from the left. For example, 'TIFF' excludes all types of TIFF file, but 'TIFF image data, little-endian' excludes only certain types of TIFF file.

## 8.4 Allowing access to multi-volume archives that can't be scanned

- ❗ A *multi-volume archive* is an archive that is split into several files. Such archives exist when there isn't enough space for the archive on a single volume (e.g. a ZIP archive that is stored on several floppy disks). Sophos Anti-Virus might not be able to scan a multi-volume archive, but you can configure Sophos Anti-Virus to allow access to such an archive anyway.

### Command line

To allow access to multi-volume archives of a particular type, use the `AllowIfMultiVolumeArchive` parameter. To see the default list of file types, type

```
/opt/sophos-av/bin/savconfig -s query AllowIfMultiVolumeArchive
```

To change the list of file types, specify either an asterisk `*` or a value that is returned by the file command. (For more information on the file command,

type `man file`.) An asterisk means any file type. For example, to add all file types to the list of file types, type

```
/opt/sophos-av/bin/savconfig AllowIfMultiVolumeArchive '*'
```

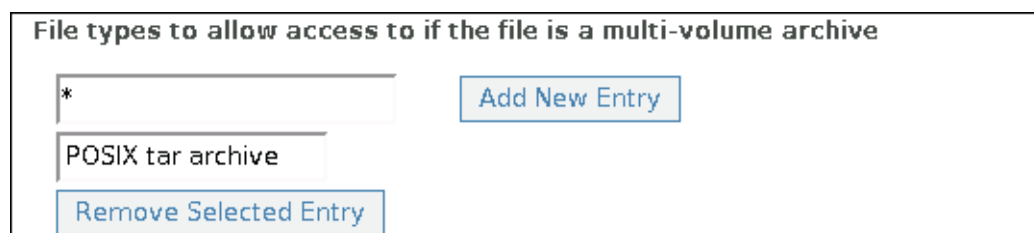
To remove a file type from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove AllowIfMultiVolumeArchive '*'
```

- ❗ Sophos Anti-Virus performs partial matching of file types. Thus, it excludes all file types that match the specified file type up to the number of characters in the specified file type, starting from the left. For example, 'TIFF' excludes all types of TIFF file, but 'TIFF image data, little-endian' excludes only certain types of TIFF file.

## GUI

To allow access to multi-volume archives of a particular type, on the **Exclusion Configuration** page, in the **Error Exclusions** panel, type the file type in the text box labeled **File types to allow access to if the file is a multi-volume archive**. The file type must be either an asterisk \* or a value that is returned by the file command. An asterisk means any file type. (For more information on the file command, type `man file`.) Click **Add New Entry** to add the file type to the list.



The screenshot shows a GUI window titled "File types to allow access to if the file is a multi-volume archive". It contains two text input fields. The first field contains an asterisk (\*). To the right of this field is a blue button labeled "Add New Entry". The second field contains the text "POSIX tar archive". Below this field is a blue button labeled "Remove Selected Entry".

To remove a file type from the list, select the file type and click **Remove Selected Entry**.

- ❗ Sophos Anti-Virus performs partial matching of file types. Thus, it excludes all file types that match the specified file type up to the number of characters in the specified file type, starting from the left. For example, 'TIFF' excludes all types of TIFF file, but 'TIFF image data, little-endian' excludes only certain types of TIFF file.

## 8.5 Excluding files and directories from scanning

### 8.5.1 Using file or directory name

#### Command line

To exclude a particular file or directory, use the `ExcludeFilePaths` parameter. For example, to add the file `/tmp/report` to the list of files and directories to exclude, type

```
/opt/sophos-av/bin/savconfig ExcludeFilePaths /tmp/report
```

To remove an exclusion from the list, use the `remove` operation. For example, type

```
/opt/sophos-av/bin/savconfig remove ExcludeFilePaths /tmp/report
```

#### GUI

To exclude a particular file or directory, on the **Exclusion Configuration** page, in the **File Scanning Exclusions** panel, type the path in the text box labeled **Files or directories (with or without wildcards)**. Click **Add New Entry** to add the path to the list.

The screenshot shows a window titled "Files or directories (with or without wildcards)". It contains two text input fields. The first field contains the path "/usr/fred/report.rtf" and has an "Add New Entry" button to its right. The second field contains the wildcard path "/tmp/\*.txt" and has a "Remove Selected Entry" button below it.

To remove an exclusion from the list, select the exclusion and click **Remove Selected Entry**.

### 8.5.2 Using file type

- ⓘ Specifying exclusions in this way means that scanning is less efficient than if you specify exclusions using file or directory name, wildcards or regular expressions.

#### Command line

To exclude files that are the same type as a specific file, use the `ExcludeFilesLike` parameter. For example, to add the type of the file `Report.txt` to the list of file types to exclude, type

```
/opt/sophos-av/bin/savconfig ExcludeFilesLike /home/fred/Report.txt
```

To remove an exclusion from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove ExcludeFilesLike
/home/fred/Report.txt
```

To exclude files that are of a specific type, use the ExcludeFileOnType parameter. The file type must be a value that is returned by the file command. (For more information on the file command, type `man file`.) For example, to add files of type ASCII text to the list of file types to exclude, type

```
/opt/sophos-av/bin/savconfig ExcludeFileOnType 'ASCII text'
```

To remove an exclusion from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove ExcludeFileOnType 'ASCII text'
```

- ⓘ Sophos Anti-Virus performs partial matching of file types. Thus, it excludes all file types that match the specified file type up to the number of characters in the specified file type, starting from the left. For example, 'TIFF' excludes all types of TIFF file, but 'TIFF image data, little-endian' excludes only certain types of TIFF file.

## GUI

To exclude files that are the same type as a specific file, on the **Exclusion Configuration** page, in the **File Scanning Exclusions** panel, type the path of the file in the text box labeled **File type of this file**. Click **Add New Entry** to add the file type to the list of file types to exclude.

**File types**

File type of this file

File type as returned by the 'file' command

To exclude files that are of a specific type, on the **Exclusion Configuration** page, in the **File Scanning Exclusions** panel, type the file type in the text box labeled **File type as returned by the 'file' command**. (For more

information on the file command, type `man file`.) Click **Add New Entry** to add the file type to the list.

**File types**

File type of this file

File type as returned by the 'file' command

To remove an exclusion from the list, select the exclusion and click **Remove Selected Entry**.

- ❗ Sophos Anti-Virus performs partial matching of file types. Thus, it excludes all file types that match the specified file type up to the number of characters in the specified file type, starting from the left. For example, 'TIFF' excludes all types of TIFF file, but 'TIFF image data, little-endian' excludes only certain types of TIFF file.

### 8.5.3 Using wildcards

#### Command line

To exclude files and directories by using wildcards, use the `ExcludeFileOnGlob` parameter. Valid wildcards are `*` which matches any number of any characters, and `?` which matches any one character. For example, to add all text files in the `/tmp` directory to the list of files and directories to exclude, type

```
/opt/sophos-av/bin/savconfig ExcludeFileOnGlob '/tmp/*.txt'
```

To remove an exclusion from the list, use the `remove` operation. For example, type

```
/opt/sophos-av/bin/savconfig remove ExcludeFileOnGlob '/tmp/*.txt'
```

#### GUI

To exclude files and directories by using wildcards, on the **Exclusion Configuration** page, in the **File Scanning Exclusions** panel, type the path in the text box labeled **Files or directories (with or without wildcards)**. Valid

wildcards are \* which matches any number of any characters, and ? which matches any one character. Click **Add New Entry** to add the path to the list.

**Files or directories (with or without wildcards)**

To remove an exclusion from the list, select the exclusion and click **Remove Selected Entry**.

### 8.5.4 Using regular expressions

#### Command line

To exclude files and directories by using regular expressions, use the ExcludeFileOnExpression parameter. To see the default list of files and directories to exclude, type

```
/opt/sophos-av/bin/savconfig -s query ExcludeFileOnExpression
```

Sophos Anti-Virus supports extended regular expressions as defined by POSIX 1003.2. (For more information on regular expressions, type man 7 regex.) For example, to add all files with filename extension .txt that are in the /tmp directory but not in subdirectories to the list of files and directories to exclude, type

```
/opt/sophos-av/bin/savconfig ExcludeFileOnExpression
'^/tmp/[^/]*\.txt$'
```

To remove an exclusion from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove ExcludeFileOnExpression
'^/tmp/[^/]*\.txt$'
```

- ❗ Sophos recommends that you include the ^ character at the beginning of the expression and the \$ character at the end. This makes the exclusion more specific, and makes it less likely that you'll exclude something that you mean to scan.

#### GUI

To exclude files and directories by using regular expressions, on the **Exclusion Configuration** page, in the **File Scanning Exclusions** panel, type the expression in the **File path regular expressions** text box. Sophos

Anti-Virus supports extended regular expressions as defined by POSIX 1003.2. (For more information on regular expressions, type `man 7 regex`.) Click **Add New Entry** to add the path to the list.

**File path regular expressions**

Add New Entry

^/tmp/[^/]\*\.txt\$

Remove Selected Entry

To remove an exclusion from the list, select the exclusion and click **Remove Selected Entry**.

- ❗ Sophos recommends that you include the `^` character at the beginning of the expression and the `$` character at the end. This makes the exclusion more specific, and makes it less likely that you'll exclude something that you mean to scan.

## 8.6 Specifying the location of magic number files

To specify the location of the magic number files that are used by the file command to determine a file's type, use the `MagicData` parameter. To see the default list of locations, type

```
/opt/sophos-av/bin/savconfig -s query MagicData
```

To add another location to the list of locations, for example type

```
/opt/sophos-av/bin/savconfig MagicData /usr/share/magic
```

To remove a location from the list, use the `remove` operation. For example, type

```
/opt/sophos-av/bin/savconfig remove MagicData /usr/share/magic
```

## 8.7 Excluding filesystems from file scanning

### Command line

To exclude filesystems from file scanning by using filesystem type, use the `ExcludeFilesystems` parameter. To see the default list of filesystem types, type

```
/opt/sophos-av/bin/savconfig -s query ExcludeFilesystems
```

Valid filesystem types are listed in the file `/proc/filesystems`. For example, to add `nfs` to the list of filesystem types to exclude, type

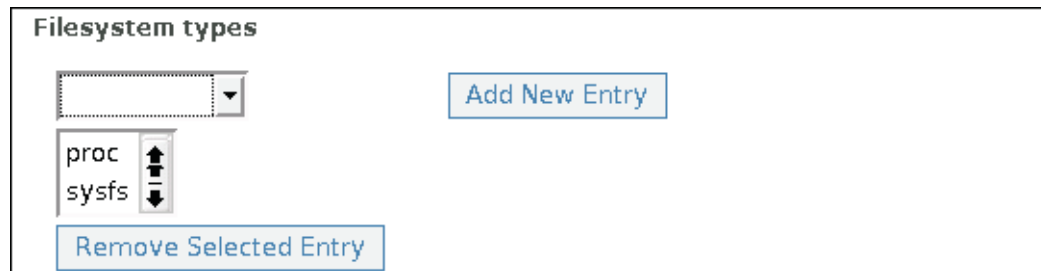
```
/opt/sophos-av/bin/savconfig ExcludeFilesystems nfs
```

To remove an exclusion from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove ExcludeFilesystems nfs
```

## GUI

To exclude filesystems from file scanning by using filesystem type, on the **Exclusion Configuration** page, in the **File Scanning Exclusions** panel, click the drop-down arrow on the box labeled **Filesystem types**. Select one of the filesystem types in the list. Click **Add New Entry** to add the filesystem type to the list.



To remove an exclusion from the list, select the exclusion and click **Remove Selected Entry**.

## 8.8 Excluding filesystems from boot sector scanning on mount

### 8.8.1 Using mount point or device name

#### Command line

To exclude filesystems from boot sector scanning when they are mounted by using mount point or device name, use the `ExcludeMountPaths` parameter. For example, to add the mount point `/mnt/infected` to the list of filesystems to exclude from boot sector scans, type

```
/opt/sophos-av/bin/savconfig ExcludeMountPaths /mnt/infected
```

and to add the device `/dev/hdd2` to the list, type

```
/opt/sophos-av/bin/savconfig ExcludeMountPaths /dev/hdd2
```

To remove an exclusion from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove ExcludeMountPaths /mnt/infected
```

## GUI

To exclude filesystems from boot sector scanning when they are mounted by using mount point or device name, on the **Exclusion Configuration** page, in the **Boot Sector Scanning Exclusions** panel, type the mount point or device name in the text box labeled **Mount points or device names**. Click **Add New Entry** to add it to the list.

The screenshot shows a window titled "Boot Sector Scanning Exclusions". Inside, there is a section labeled "Mount points or device names". Below this label is a text input field containing the text "/mnt/savcd". To the right of the input field is a blue button with the text "Add New Entry". Below the input field is another blue button with the text "Remove Selected Entry".

To remove an exclusion from the list, select the exclusion and click **Remove Selected Entry**.

### 8.8.2 Using filesystem type

To exclude filesystems from boot sector scanning when they are mounted by using filesystem type, use the ExcludeBootSectorScans parameter. Valid filesystem types are listed in the file /proc/filesystems. For example, to add ext3 to the list of filesystem types to exclude from boot sector scanning, type

```
/opt/sophos-av/bin/savconfig ExcludeBootSectorScans ext3
```

To remove an exclusion from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove ExcludeBootSectorScans ext3
```

### 8.8.3 Using regular expressions for mount point

To exclude filesystems from boot sector scanning when they are mounted by using regular expressions for mount point, use the ExcludeMountpointExpression parameter. Sophos Anti-Virus supports extended regular expressions as defined by POSIX 1003.2. (For more

information on regular expressions, type `man 7 regex`.) For example, to exclude the mount point `/mnt/infected`, type

```
/opt/sophos-av/bin/savconfig ExcludeMountpointExpression  
'^/mnt/infected$'
```

To remove an exclusion from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove ExcludeMountpointExpression  
'^/mnt/infected$'
```

- ❗ Sophos recommends that you include the `^` character at the beginning of the expression and the `$` character at the end. This makes the exclusion more specific, and makes it less likely that you'll exclude something that you mean to scan.

#### 8.8.4 Using regular expressions for device name

To exclude filesystems from boot sector scanning when they are mounted by using regular expressions for device name, use the `ExcludeDeviceExpression` parameter. Sophos Anti-Virus supports extended regular expressions as defined by POSIX 1003.2. (For more information on regular expressions, type `man 7 regex`.) For example, to exclude the device `/dev/hdd2`, type

```
/opt/sophos-av/bin/savconfig ExcludeDeviceExpression '^/dev/hdd2$'
```

To remove an exclusion from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove ExcludeDeviceExpression  
'^/dev/hdd2$'
```

- ❗ Sophos recommends that you include the `^` character at the beginning of the expression and the `$` character at the end. This makes the exclusion more specific, and makes it less likely that you'll exclude something that you mean to scan.

## 8.9 Scanning within archives

- ❗ Scanning within archive files makes scanning significantly slower and is rarely required. Even if you don't enable the option, when you attempt to access a file extracted from an archive file, the extracted file is scanned.

### Command line

To enable scanning within archives, type

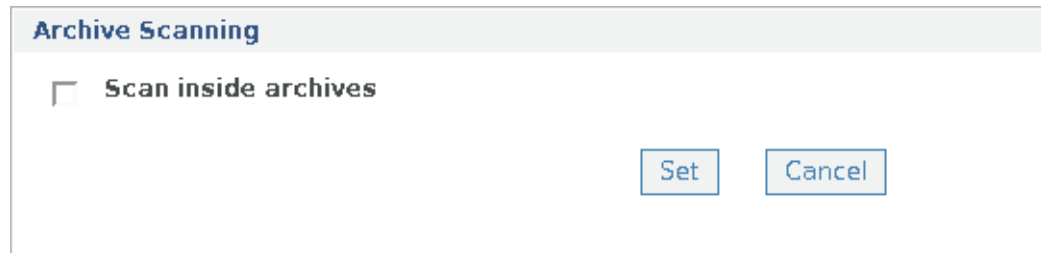
```
/opt/sophos-av/bin/savconfig set SaviGroup.Archives enabled
```

To disable scanning within archives, type

```
/opt/sophos-av/bin/savconfig set SaviGroup.Archives disabled
```

## GUI

To configure scanning within archives, go to the **Scanning Configuration** page, **Archive Scanning** panel.



Configure scanning within archives as described below. When you have done this, click **Set** to apply the changes. To undo any changes that you have made since you last clicked **Set**, click **Cancel**.

To enable scanning within archives, select the **Scan inside archives** check box.

To disable scanning within archives, clear the **Scan inside archives** check box.

## 8.10 Specifying filesystem types for which successful scans are cached

Sophos Anti-Virus uses Decision Caching technology to maintain a cache of the files that it has successfully scanned. Therefore, when you try to access a file, if Sophos Anti-Virus has previously scanned it and found it to be clean, and if it hasn't changed since the previous scan, Sophos Anti-Virus allows access without rescanning it. Thus, access to the file is faster.

Sophos Anti-Virus maintains the cache for only certain filesystem types. To see which types are included by default, type

```
/opt/sophos-av/bin/savconfig -s query CacheFileSystems
```

To change the list of filesystem types, use the CacheFileSystems parameter. Valid filesystem types are listed in the file `/proc/filesystems`. For example, to add `ext3` to the list of filesystem types, type

```
/opt/sophos-av/bin/savconfig CacheFileSystems ext3
```

To remove a filesystem from the list, use the remove operation. For example, type

```
/opt/sophos-av/bin/savconfig remove CacheFilesystems ext3
```

- ❗ It is important that network and other shared filesystem types are not included in this list. This is because Sophos Anti-Virus cannot maintain the cache for files that are stored on other computers or might be modified without access via this computer.

## 9 Configuring on-demand scanning

In this section, where PATH appears in a command, it refers to the path to be scanned.

### 9.1 Scanning all file types

By default, Sophos Anti-Virus scans executable files only. To scan all files, irrespective of their type, type

```
savscan PATH -all
```

- ❗ This takes longer than scanning only executables, and can compromise performance on servers when Sophos Anti-Virus tries to open files already in use. It can also cause false virus reports.

### 9.2 Scanning inside archives

Sophos Anti-Virus can scan inside archives if it is run with the `-archive` option.

```
savscan PATH -archive
```

Archive types that can be scanned include: ARJ, CMZ, GZip, RAR, TAR, Zip.

Archives 'nested' within other archives (e.g. a TAR archive within a Zip archive) are scanned recursively.

Alternatively, you can specify scanning of particular types of archive. For example, to scan inside TAR archives, type

```
savscan PATH -tar
```

or to scan inside TAR and Zip archives, type

```
savscan PATH -tar -zip
```

If you have numerous complex archives, the scan may take longer to run. Bear this in mind when scheduling unattended scans.

For a full list of the archive types scanned, use the `-vv` option.

## 9.3 Scanning remote computers

By default, Sophos Anti-Virus does not scan items on remote computers (i.e. does not traverse remote mount points). To enable scanning of remote computers, type

```
savscan PATH --no-stay-on-machine
```

## 9.4 Disabling scanning of symbolically linked items

By default, Sophos Anti-Virus scans symbolically linked items. To disable this type of scanning, type

```
savscan PATH --no-follow-symlinks
```

To avoid scanning items more than once, use the `--backtrack-protection` option.

## 9.5 Scanning the starting filesystem only

Sophos Anti-Virus can be configured not to scan items that are beyond the starting filesystem (i.e. not to traverse mount points). Type

```
savscan PATH --stay-on-filesystem
```

## 9.6 Command-line options

The command-line options listed in this section enable you to configure scanning and disinfection. There are

- options that Sophos Anti-Virus for Linux has in common with Sophos Anti-Virus for non-Linux/UNIX platforms (section 9.6.1)
- options that Sophos Anti-Virus for Linux has in common with Sophos Anti-Virus for UNIX (section 9.6.2)
- options specific to Sophos Anti-Virus for Linux (section 9.6.3).

### 9.6.1 Sophos Anti-Virus command-line options

To invert the meaning of a command-line option, prefix it with 'n'. For example, `-nsc` is the inverse of `-sc`.

For a listing of these options on screen, type

```
savscan -h
```

**-all Scan all files**

If this option is used, Sophos Anti-Virus will scan all files in a filesystem, rather than just the executable files.

- ❗ This takes longer than scanning only executables, and can compromise performance on servers when Sophos Anti-Virus tries to open files already in use. It can also cause false virus reports.

**-archive Scan inside archives**

If this option is used, Sophos Anti-Virus scans inside archives. The archive types scanned include ARJ, CMZ, GZip, RAR, TAR, Zip.

Archives 'nested' within other archives (e.g. a TAR archive within a Zip archive) are scanned recursively.

Alternatively, you can specify scanning of particular types of archive. For example, to scan inside TAR archives, type

```
savscan PATH -tar
```

or to scan inside TAR and Zip archives, type

```
savscan PATH -tar -zip
```

If you have numerous complex archives, the scan may take longer to run. Bear this in mind when scheduling unattended scans.

For a full list of the archive types scanned, use the -vv option.

**-b Sound bell on virus detection**

This option directs Sophos Anti-Virus to sound a bell when a virus or virus fragment is discovered. It is enabled by default.

**-c Ask for confirmation before disinfection or deletion**

This option directs Sophos Anti-Virus to ask for confirmation before disinfecting or deleting files. It is enabled by default.

**-di Disinfect**

This option enables Sophos Anti-Virus to perform automatic disinfection of data files, programs and boot sectors. Refer to [section 5.3](#).

**-dn Display names of files as they are scanned**

This option displays files being scanned. The display consists of the time followed by the item being checked.

**-eec Use extended set of error codes**

This option directs Sophos Anti-Virus to use an extended set of error codes. For details, refer to [section 3.6.1](#).

**-exclude Exclude items from scanning**

This option enables you to specify that any items (files, directories or filesystems) that follow the option on the command line must be excluded from scanning.

After using the option `-exclude`, you can use the option `-include` to specify that items that follow this option on the command line must be scanned.

For example

```
savscan fred harry -exclude tom peter -include bill
```

scans items fred, harry and bill, but not tom or peter.

The option `-exclude` can be used for files or directories under another directory. For example

```
savscan /home/fred -exclude /home/fred/games
```

scans all of Fred's home directory, but excludes the directory games (and all directories and files under it).

**-ext= File types defined as executables**

By default, Sophos Anti-Virus scans DOS and Windows executable files with certain file extensions (run `savscan` with the `-vv` qualifier to see a list of the file extensions used).

To specify additional file extensions that Sophos Anti-Virus will scan, use the `-ext=` option with a comma-separated list of extensions.

To exempt file extensions from scanning, use `-next`.

 If you want to scan files that UNIX defines as executables, refer to the `examine-x-bit` qualifier in [section 9.6.2](#).

**-f Full scan**

By default, Sophos Anti-Virus checks only those parts of each file that are likely to contain viruses. A 'full' scan examines the complete contents of each file and can be specified using this option.

Full scanning is slower than default scanning.

**-h Help**

This option lists all the command-line options, including Linux-specific options.

**-idedir= Use alternative directory for virus identity files (IDEs)**

This option enables you to specify an alternative directory for IDEs. For example

```
savscan PATH -idedir=/ide
```

directs Sophos Anti-Virus to read IDEs from the `/ide` directory instead of the default directory (normally `/opt/sophos-av/lib/sav`).

**-mime Scan MIME files**

This option enables Sophos Anti-Virus to scan MIME files when it does a scan. By default, it is *not* enabled to scan MIME files.

**-oe Scan Outlook Express mailboxes**

This option directs Sophos Anti-Virus to scan Outlook Express mailboxes when it does a scan. By default, it is *not* enabled to scan Outlook Express mailboxes. You must also use the `-mime` option with this qualifier.

**-p= <file|device> Copy screen output to file or device**

This option directs Sophos Anti-Virus to send whatever it sends to the screen to a particular file or device as well. For example

```
savscan PATH -p=log.txt
```

directs Sophos Anti-Virus to send screen output to the file `log.txt`.

**-rec Do recursive scan**

This option directs Sophos Anti-Virus to scan directories below the ones specified in the command line. It is enabled by default.

**-remove Remove infected objects**

This option directs Sophos Anti-Virus to remove infected items.

**-s Silent running without displaying checked areas**

If this option is used, Sophos Anti-Virus does not display on the screen the files it is scanning. It is enabled by default.

### **-sc Scan inside compressed files**

If this option is used, Sophos Anti-Virus looks for viruses inside files compressed with PKLite, LZEXE and Diet. It is enabled by default.

### **--stop-scan Stop scanning “zip bombs”**

If this option is used, Sophos Anti-Virus stops scanning “zip bombs” when they are detected.

- ❓ “Zip bombs” are malicious files that are designed to disrupt the action of anti-virus scanners. These files usually take the form of innocent looking archive files that, when unpacked in order to be scanned, require enormous amounts of time, disk space, or memory.

For example

```
savscan -all /home/fred/misc --stop-scan
```

directs Sophos Anti-Virus to scan all objects (files and directories) under /home/fred/misc, and to stop scanning any “zip bombs” that are detected. When a “zip bomb” is detected, a message such as

```
Aborted checking /home/fred/misc/b.zip - appears to  
be a 'zip bomb'
```

is displayed.

### **-v Version number**

If this option is used, Sophos Anti-Virus displays the version number and a list of the virus identities (IDEs) currently in use.

### **-vv Full version information**

If this option is used, Sophos Anti-Virus displays the version number and lists of the virus identities (IDEs) currently in use, the file extensions that are scanned, and the archive types scanned.

## 9.6.2 UNIX-specific command-line options

The following options are UNIX-specific, and may be prefixed with 'no-' to invert their meaning.

For example, '--no-follow-symlinks' is the inverse of '--follow-symlinks'.

### **--args-file=[filename] Read command-line arguments from file**

Sophos Anti-Virus reads command-line arguments from a file. The arguments may include (lists of) directory names, filenames and options. For example

```
savscan --args-file=scanlist
```

directs Sophos Anti-Virus to read command-line arguments from the `scanlist` file. When Sophos Anti-Virus reaches the end of the file, it continues reading arguments from the command line.

If [filename] is '-', Sophos Anti-Virus reads arguments from stdin. Some command-line options may not be used in the file: -eec, -neec, -p=, -s, -ns, -dn and -ndn.

### **--backtrack-protection Prevent backtracking**

Sophos Anti-Virus avoids scanning the same files more than once ('backtracking'), a problem that can arise due to symbolic links. This option is enabled by default.

### **--examine-x-bit Scan all items that UNIX defines as executables**

If this option is used, Sophos Anti-Virus scans all items that UNIX defines as executables, as well as items with the file extensions in Sophos Anti-Virus's own executables list (for details of the file extensions listed, run `savscan` with the -vv qualifier).

### **--follow-symlinks Scan the object pointed to by symbolic links**

Sophos Anti-Virus scans objects pointed to by symbolic links. This option is enabled by default.

### **--preserve-backtrack Preserve backtracking information**

Sophos Anti-Virus preserves the backtracking information for the duration of the run. This option is enabled by default.

### **--quarantine Quarantine infected files**

If this option is used, Sophos Anti-Virus puts infected files into quarantine. Sophos Anti-Virus does this by changing the ownership and permissions for the file.

If you have specified disinfection, Sophos Anti-Virus attempts to disinfect the file and quarantines the file only if disinfection fails.

Unless you specify otherwise, Sophos Anti-Virus changes the ownership of the file to that of the user running Sophos Anti-Virus and changes the file permissions to `-r -r----- (0400)`.

You can use the option with further parameters:

```
uid=NNN
user=USERNAME
gid=NNN
group=GROUP-NAME
mode=PPP
```

You cannot specify more than one parameter of each type (e.g. you cannot enter username twice, or enter a uid and a username).

For each parameter you do not specify, the default setting (as given above) is used.

For example:

```
savscan fred -quarantine:user=sophosav,group=virus,mode=0400
```

will change an infected file's user ownership to `sophosav`, the group ownership to `virus`, and the file permissions to `-r-----`. This means the file is owned by the user `sophosav` and group `virus`, but *only* the user `sophosav` can access the file (and only for reading). No one else can do anything to the file (apart from root).

You may need to be running as a special user or as superuser to set the ownership and permissions.

### **--reset-atime Reset the access time on files**

After Sophos Anti-Virus scans a file, it resets the access time (the `atime`) to the time shown before scanning. However, if a file is disinfected, the access and modification times are updated. This option is enabled by default.

- 🔗 You may find that your archiver always backs up all the files that have been scanned. This could happen because resetting the `atime` has the effect of changing the inode status-changed time (`ctime`). In this case, run `savscan` with the `--no-reset-atime` option.

**--show-file-details Show details of file ownership**

If this option is used, Sophos Anti-Virus shows details of the file ownership and permissions when filenames are displayed or written to a log.

**--skip-special Do not scan 'special' objects**

Sophos Anti-Virus does not scan special objects, such as /dev, /proc, /devices etc. This option is enabled by default.

**--stay-on-filesystem Attempt not to leave the starting filesystem**

If this option is used, Sophos Anti-Virus scans only the starting filesystem, i.e. it does not traverse mount points.

**--stay-on-machine Attempt not to leave the starting computer**

Sophos Anti-Virus scans only the starting computer, i.e. it does not traverse remote mount points. This option is enabled by default.

### 9.6.3 Linux-specific command-line options

The following boot sector scanning options are only available with Sophos Anti-Virus for Linux.

**-bs=xxx, xxx,... Scan boot sector of specific logical drive**

Sophos Anti-Virus scans the boot sectors of specified logical drives, where xxx is the name of the drive (for example /dev/fd0 or /dev/hda1). The floppy drive is considered a logical device for the purposes of this option.

You can use this option to scan the boot sectors of floppy disks that were created for other operating systems (e.g. Windows and DOS).

**-bs Scan all known boot sectors**

Sophos Anti-Virus extracts partition table information from all the physical drives it knows about, then scans all logical drive boot sectors. This includes boot sectors that are not Linux (e.g. Windows and DOS).

**-cdr= Scan CD boot image**

To scan the boot image of a bootable CD, use the -cdr option. For example

```
savscan -cdr=/dev/cdrom
```

scans the boot image (if any) of the CD on device /dev/cdrom. If Sophos Anti-Virus finds a boot image, it scans the boot sector of that image for boot sector viruses.

To scan for program viruses all files in the boot image whose file type is in Sophos Anti-Virus's own executables list, use the `-loopback` option. For example

```
savscan -cdr=/dev/cdrom -loopback
```

scans the boot image (if any) of the CD on device `/dev/cdrom`. If Sophos Anti-Virus finds a boot image, it scans the boot sector of that image for boot sector viruses and scans for program viruses all files in that image whose file type is in the executables list.

**-mbr Scan master boot records**

Sophos Anti-Virus attempts to scan the master boot records for all the physical drives on the system.

## 10 Configuring alerts

- ❗ If you are configuring a single computer that is on a network, such configuration might be discarded if the computer downloads a new corporate configuration.

You can configure Sophos Anti-Virus to send an alert when it finds a virus, there is a scanning error or some other type of error. Alerts can be sent in different languages, and via the following methods:

- Desktop pop-ups (on-access scanning only)
- Command-line alerts (on-access scanning only)
- Email alerts (on-access and on-demand scanning)

### 10.1 Configuring desktop pop-up alerts

By default, desktop pop-up alerts are enabled.

#### Command line

To enable desktop pop-up alerts, set the parameters `UINotifier` and `UIpopupNotification` to “enabled”. `UINotifier` provides overall control of desktop pop-up and command-line alerts; `UIpopupNotification` controls just desktop pop-up alerts. For example, type

```
/opt/sophos-av/bin/savconfig UINotifier enabled
/opt/sophos-av/bin/savconfig UIpopupNotification enabled
```

You can specify what message is sent in addition to the alert itself, and the locale of the computers that receive the message. (For a list of the locales that you can specify, refer to [Appendix 1](#).) Default messages are supplied for English and Japanese. To change one of these, or add a message for another locale, use the parameter `UIContactMessage` and specify the locale. For example, type

```
/opt/sophos-av/bin/savconfig UIContactMessage en 'Contact IT'
```

- ❗ The same messages are used for desktop pop-up and command-line alerts.

To disable desktop pop-up alerts, type

```
/opt/sophos-av/bin/savconfig UIpopupNotification disabled
```

To disable both desktop pop-up and command-line alerts, type

```
/opt/sophos-av/bin/savconfig UINotifier disabled
```

## GUI

To configure desktop pop-up alerts, go to the **Alerts Configuration** page, **Desktop Pop-up and Command-line** panel.

**Desktop Pop-up and Command-line**

Enable desktop pop-up alerts

Enable command-line alerts

**Additional message to be displayed in command-line and desktop pop-up alerts**

English en

Please contact your IT department.

Remove

Japanese ja

IT 部門にお問い合わせください。

Remove

Add New Entry

Set Cancel

Configure desktop pop-up alerts as described below. When you have done this, click **Set** to apply the changes. To undo any changes that you have made since you last clicked **Set**, click **Cancel**.

To enable desktop pop-up alerts, select the **Enable desktop pop-up alerts** check box.

You can specify what message is sent in addition to the alert itself, and the locale of the computers that receive the message. (For a list of the locales that you can specify, refer to [Appendix 1](#).) The GUI displays a list of messages for different locales. Default messages are supplied for English and Japanese.

To change the locale of an existing message, select the locale in the drop-down list box. To edit the text of an existing message in the list, type in the message box.

To add a new message to the list, select the locale in the drop-down list box, type the text in the message box and click **Add New Entry**.

To delete a message from the list, click the **Remove** button to the right of the message.

- 🔗 The same messages are used for desktop pop-up and command-line alerts.

To disable desktop pop-up alerts, clear the **Enable desktop pop-up alerts** check box.

## 10.2 Configuring command-line alerts

By default, command-line alerts are enabled.

### Command line

To enable command-line alerts, set the parameters `UINotifier` and `UIttyNotification` to “enabled”. `UINotifier` provides overall control of desktop pop-up and command-line alerts; `UIttyNotification` controls just command-line alerts. For example, type

```
/opt/sophos-av/bin/savconfig UINotifier enabled
/opt/sophos-av/bin/savconfig UIttyNotification enabled
```

You can specify what message is sent in addition to the alert itself, and the locale of the computers that receive the message. (For a list of the locales that you can specify, refer to [Appendix 1](#).) Default messages are supplied for English and Japanese. To change one of these, or add a message for another locale, use the parameter `UIContactMessage` and specify the locale. For example, type

```
/opt/sophos-av/bin/savconfig UIContactMessage en 'Contact IT'
```

- 🔗 The same messages are used for desktop pop-up and command-line alerts.

To disable command-line alerts, type

```
/opt/sophos-av/bin/savconfig UIttyNotification disabled
```

To disable both desktop pop-up and command-line alerts, type

```
/opt/sophos-av/bin/savconfig UINotifier disabled
```

## GUI

To configure command-line alerts, go to the **Alerts Configuration** page, **Desktop Pop-up and Command-line** panel.

**Desktop Pop-up and Command-line**

Enable desktop pop-up alerts

Enable command-line alerts

**Additional message to be displayed in command-line and desktop pop-up alerts**

English en

Please contact your IT department.

Remove

Japanese ja

IT 部門にお問い合わせください。

Remove

Add New Entry

Set Cancel

Configure command-line alerts as described below. When you have done this, click **Set** to apply the changes. To undo any changes that you have made since you last clicked **Set**, click **Cancel**.

To enable command-line alerts, select the **Enable command-line alerts** check box.

You can specify what message is sent in addition to the alert itself, and the locale of the computers that receive the message. (For a list of the locales that you can specify, refer to [Appendix 1](#).) The GUI displays a list of messages for different locales. Default messages are supplied for English and Japanese.

To change the locale of an existing message in the list, select the locale in the drop-down list box. To edit the text of an existing message in the list, type in the message box.

To add a new message to the list, select the locale in the drop-down list box, type the text in the message box and click **Add New Entry**.

To delete a message from the list, click the **Remove** button to the right of the message.

 The same messages are used for desktop pop-up and command-line alerts.

To disable command-line alerts, clear the **Enable command-line alerts** check box.

### 10.3 Configuring email alerts

By default, email alerts are

- enabled
- sent when a virus is detected or there is a scanning error
- sent only when there is a fatal event
- sent to root@localhost

and the hostname and port of the SMTP server are localhost:25.

#### Command line

To enable email alerts, set the parameter EmailNotifier to “enabled”:

```
/opt/sophos-av/bin/savconfig EmailNotifier enabled
```

To set the hostname or IP address of the SMTP server, use the parameter EmailServer. For example, type

```
/opt/sophos-av/bin/savconfig EmailServer 171.17.31.184
```

To enable email alerts to be sent when a virus is detected, set the parameter SendThreatEmail to “enabled”:

```
/opt/sophos-av/bin/savconfig SendThreatEmail enabled
```

To enable email alerts to be sent when there is a scanning error, set the parameter SendErrorMessage to “enabled”:

```
/opt/sophos-av/bin/savconfig SendErrorMessage enabled
```

You can also specify which types of event generate an email alert by using the parameter `SendEmailLogLevel`. Valid values are:

FATAL	Only fatal events generate an email alert.
ERROR	Less serious as well as FATAL events generate an email alert.
NOTICE	Trivial as well as ERROR events generate an email alert.

To specify who receives email alerts, use the parameter `Email` and specify the locale of the email recipients. (For a list of the locales that you can specify, refer to [Appendix 1.](#)) You can specify more than one recipient. For example, type

```
/opt/sophos-av/bin/savconfig Email en admin@localhost
```

You can specify what message is sent in addition to the alert itself when a *virus is detected*, and the locale of the email recipients. (For a list of the locales that you can specify, refer to [Appendix 1.](#)) Default messages are supplied for English and Japanese. To change one of these, or add a message for another locale, use the parameter `ThreatMessage` and specify the locale. For example, type

```
/opt/sophos-av/bin/savconfig ThreatMessage en 'Contact IT'
```

You can specify what message is sent in addition to the alert itself when *there is a scanning error*, and the locale of the email recipients. (For a list of the locales that you can specify, refer to [Appendix 1.](#)) Default messages are supplied for English and Japanese. To change one of these, or add a message for another locale, use the parameter `ScanErrorMessage` and specify the locale. For example, type

```
/opt/sophos-av/bin/savconfig ScanErrorMessage en 'Contact IT'
```

You can specify what message is sent in addition to the alert itself when *an event is logged in the Sophos Anti-Virus log*, and the locale of the email recipients. (For a list of the locales that you can specify, refer to [Appendix 1.](#)) Default messages are supplied for English and Japanese. To change one of these, or add a message for another locale, use the parameter `LogMessage` and specify the locale. For example, type

```
/opt/sophos-av/bin/savconfig LogMessage en 'Contact IT'
```

To disable email alerts, type

```
/opt/sophos-av/bin/savconfig EmailNotifier disabled
```

## GUI

To configure email alerts via the GUI, go to the **Alerts Configuration** page, **Email** panel.



The screenshot shows a configuration window with a checked checkbox labeled "Enable email alerts". Below it is a label "Hostname or IP address of the SMTP server" and a text input field containing "localhost:25". At the bottom right are two buttons: "Set" and "Cancel".

To enable email alerts, select the **Enable email alerts** check box.

To set the hostname or IP address of the SMTP server, type the address in the text box labeled **Hostname or IP address of the SMTP server**.

To disable email alerts, clear the **Enable email alerts** check box.

When you have finished configuring email alerts, click **Set** to apply the changes. To undo any changes that you have made since you last clicked **Set**, click **Cancel**.

The screenshot shows a window titled "Email recipients". At the top is a dropdown menu with "English en" selected. Below it is a text input field containing "root@localhost". To the right of this field is a blue button labeled "Remove". Below the input field is another dropdown menu. At the bottom right of the window is a blue button labeled "Add New Entry".

You can specify who receives email alerts, and the locale of the email recipients. (For a list of the locales that you can specify, refer to [Appendix 1](#).) The GUI displays a list of email recipients for different locales, under **Email recipients**.

To change the locale of an existing email recipient in the list, select the locale in the drop-down list box. To edit the address of an existing email recipient in the list, type in the address box.

To add a new email recipient to the list, select the locale in the drop-down list box, type the text in the address box and click **Add New Entry**.

To delete an email recipient from the list, click the **Remove** button to the right of the recipient.

When you have finished configuring email alerts, click **Set** to apply the changes. To undo any changes that you have made since you last clicked **Set**, click **Cancel**.

**Send email when virus detected**

**Additional message to be included in virus detection email alerts**

English en	
Please contact your IT department.	Remove
Japanese ja	
IT 部門にお問い合わせください。	Remove
	Add New Entry

To enable email alerts to be sent when *a virus is detected*, select the check box labeled **Send email when virus detected**.

You can specify what message is sent in addition to the alert itself when a virus is detected, and the locale of the email recipients. (For a list of the locales that you can specify, refer to [Appendix 1](#).) The GUI displays a list of messages for different locales. Default messages are supplied for English and Japanese.

To change the locale of an existing message in the list, select the locale in the drop-down list box. To edit the text of an existing message in the list, type in the message box.

To add a new message to the list, select the locale in the drop-down list box, type the text in the message box and click **Add New Entry**.

To delete a message from the list, click the **Remove** button to the right of the message.

When you have finished configuring email alerts, click **Set** to apply the changes. To undo any changes that you have made since you last clicked **Set**, click **Cancel**.

**Send email when there is a scan error**

**Additional message to be included in scan error email alerts**

English en

Please contact your IT department.

Remove

Japanese ja

IT 部門にお問い合わせください。

Remove

Add New Entry

To enable email alerts to be sent when *there is a scanning error*, select the check box labeled **Send email when there is a scan error**.

You can specify what message is sent in addition to the alert itself when there is a scanning error, and the locale of the email recipients. (For a list of the locales that you can specify, refer to [Appendix 1](#).) The GUI displays a list of messages for different locales. Default messages are supplied for English and Japanese.

To change the locale of an existing message in the list, select the locale in the drop-down list box. To edit the text of an existing message in the list, type in the message box.

To add a new message to the list, select the locale in the drop-down list box, type the text in the message box and click **Add New Entry**.

To delete a message from the list, click the **Remove** button to the right of the message.

When you have finished configuring email alerts, click **Set** to apply the changes. To undo any changes that you have made since you last clicked **Set**, click **Cancel**.

**Additional message to be included in log event email alerts**

English en	
Please contact your IT department.	Remove
Japanese ja	
IT 部門にお問い合わせください。	Remove
	Add New Entry

You can specify what message is emailed when *an event is logged in the Sophos Anti-Virus log*, and the locale of the email recipients. (For a list of the locales that you can specify, refer to [Appendix 1](#).) The GUI displays a list of messages for different locales. Default messages are supplied for English and Japanese.

To change the locale of an existing message in the list, select the locale in the drop-down list box. To edit the text of an existing message in the list, type in the message box.

To add a new message to the list, select the locale in the drop-down list box, type the text in the message box and click **Add New Entry**.

To delete a message from the list, click the **Remove** button to the right of the message.

When you have finished configuring email alerts, click **Set** to apply the changes. To undo any changes that you have made since you last clicked **Set**, click **Cancel**.

## 11 Configuring the Sophos Anti-Virus log

- ❗ If you are configuring a single computer that is on a network, such configuration might be discarded if the computer downloads a new corporate configuration.

By default, scanning activity is logged in the Sophos Anti-Virus log. However, to disable this, set the parameter `LogNotifier` to “disabled”:

```
/opt/sophos-av/bin/savconfig LogNotifier disabled
```

This will still allow scanning activity to be logged in `syslog`.

When a virus is detected or there is a scanning error, Sophos Anti-Virus logs the event and also logs a standard message. You can specify what this standard message is, and the locale of the message. (For a list of the locales that you can specify, refer to [Appendix 1](#).) Default messages are supplied for English and Japanese. To change one of these, or add a message for another locale, use the parameter `LogMessage` and specify the locale. For example, type

```
/opt/sophos-av/bin/savconfig LogMessage en 'Contact IT'
```

When the Sophos Anti-Virus log reaches a particular size, it is backed up automatically and a new log is started. To see the default maximum size, type

```
/opt/sophos-av/bin/savconfig -s query LogMaxSizeMB
```

To specify the maximum size of the log, set the parameter `LogMaxSizeMB` to the file size in megabytes. For example, type

```
/opt/sophos-av/bin/savconfig LogMaxSizeMB 50
```

## 12 Configuring the Sophos Anti-Virus GUI

- ❗ If you are configuring a single computer that is on a network, such configuration might be discarded if the computer downloads a new corporate configuration.

You can configure the Sophos Anti-Virus GUI using either

- the utility `savsetup`, or
- the command `savconfig`.

### **savsetup**

1. At the computer, run the utility `savsetup`, which is in the `bin` subdirectory of the installation:

```
/opt/sophos-av/bin/savsetup
```

2. The utility asks you to select what you want to do. Select **Sophos Anti-Virus GUI configuration**.
3. The utility asks you a series of questions about the GUI. Type your responses to configure the GUI.

### **savconfig**

To set the http port on which the GUI runs, use the parameter `HttpPort`. (The GUI is not accessible via an *external* port.) To see the default port, type

```
/opt/sophos-av/bin/savconfig -s query HttpPort
```

To change the port, type for example

```
/opt/sophos-av/bin/savconfig HttpPort 1880
```

To set the username, use the parameter `HttpUsername`. For example, type

```
/opt/sophos-av/bin/savconfig HttpUsername sysadmin
```

To set the password, use the parameter `HttpPassword`. For example, type

```
/opt/sophos-av/bin/savconfig HttpPassword 0jf09jf
```

These settings don't take effect until the GUI daemon is restarted. To do this manually, close the GUI and, at the command line, type

```
/etc/init.d/sav-web restart
```



# ***Updating Sophos Anti-Virus***

**Updating Sophos Anti-Virus immediately**

**Kernel support**

**Configuring updating**

## **13 Updating Sophos Anti-Virus immediately**

Provided that you have enabled auto-updating, Sophos Anti-Virus is kept updated automatically.

To update a computer between regular updates, run the update script:

```
/opt/sophos-av/bin/savupdate
```

## 14 Kernel support

### 14.1 Support for new kernel releases

When one of the Linux vendors supported by Sophos Anti-Virus releases an update to its Linux kernel, Sophos releases an update to the Sophos kernel interface module to support this. If you apply a Linux kernel update *before* you apply the matching Sophos kernel interface module update, on-access scanning is disabled and an error is reported.

To avoid this problem, you must confirm that the matching Sophos kernel interface module update has been released before applying the Linux kernel update. A list of supported Linux distributions and updates is available on the Sophos website ([www.sophos.com](http://www.sophos.com)). When the required Sophos kernel interface module update is listed, it is available for download. Provided that you have enabled auto-updating, Sophos Anti-Virus downloads the update automatically. Alternatively, to update a computer between regular updates, run the update script:

```
/opt/sophos-av/bin/savupdate
```

You can then apply the Linux kernel update.

### 14.2 Support for customized kernels

If you customize your Linux kernels, this manual doesn't explain how to configure updating to support this. Refer to Sophos support knowledgebase article 3503 ([www.sophos.com/support/knowledgebase/article/3503.html](http://www.sophos.com/support/knowledgebase/article/3503.html)).

# 15 Configuring updating

## 15.1 Basic concepts

### Update server

An *update server* is a computer on which Sophos Anti-Virus is installed and which also acts as an update source for other computers.

### Update endpoint

An *update endpoint* is a computer on which Sophos Anti-Virus is installed and which doesn't need to act as an update source for other computers.

### Update groups

Update configuration is organised into *update groups*. Every computer that updates automatically is assigned to an update group, so that all the computers in that group have the same update configuration. If you have a complex network, you can set up different update groups for different groups of computers. You might do this because you want to update different groups of computers from different update sources.

### Packages

Within each update group, there are one or more *packages*. A package relates to a particular version of Sophos Anti-Virus from which you want to update. This facility is really for the situation where you customize your Linux kernels, and you want to control when you start updating from the latest version. If you don't do this, there is usually only *one* package in an update group, which relates to the *latest* version.

### Update source

Each package updates from a particular *update source*. This is the location of the updates. It might need access credentials.

### Update cache (cached package files)

The *update cache* is a local copy of some or all of the package on the computer(s) where Sophos Anti-Virus is installed. It is from this that the running copy of Sophos Anti-Virus is updated on the computer(s).

### Update vendors

If a computer is acting as an update server, you must specify which Linux distributions it must be able to provide updates for. These are the *update vendors*.

## 15.2 Configuring updating for a network

If you installed Sophos Anti-Virus across a network, you can set parameters of one or more update groups centrally. Then, at each computer, you can assign that computer to an update group.

You can check the current update group configuration for the network (section 15.2.1). Then, either

- add a new update group (section 15.2.2) or
- configure an existing update group (section 15.2.3).

Then, assign computers to the update group (section 15.2.4).

### 15.2.1 Checking the update group configuration for the network

Details of the update groups are stored in the corporate configuration file. (For more information about this file, refer to [section 7.3](#).) To check the current configuration, do as follows:

1. Go to the computer where you created the corporate configuration file.
2. Run the utility `savsetup`, which is in the `bin` subdirectory of the installation. Specify the path of the offline corporate configuration file (represented here by `CONFIG-FILE`) and that you are accessing the corporate layer of this file:

```
/opt/sophos-av/bin/savsetup --configfile=CONFIG-FILE --corporate
```

3. The utility asks you to select what you want to do. Select **Updating configuration**.
4. The utility asks you to select what you want to do. Select **Display update configuration** to see the current configuration.

### 15.2.2 Adding a new update group

Details of the update groups are stored in the corporate configuration file. (For more information about this file, refer to [section 7.3](#).) To add a new update group to the corporate configuration file, do as follows:

1. Go to the computer where you created the corporate configuration file.
2. Run the utility `savsetup`, which is in the `bin` subdirectory of the installation. Specify the path of the offline corporate configuration file (represented here by `CONFIG-FILE`) and that you are accessing the corporate layer of this file:

```
/opt/sophos-av/bin/savsetup --configfile=CONFIG-FILE --corporate
```

3. The utility asks you to select what you want to do. Select **Updating configuration**.

4. The utility asks you to select what you want to do. Select **Add new update group**.
5. The utility asks you for a name for the update group. Type a name for the group.
6. The utility asks you what website or directory the package should be downloaded from. This is the update source. Type the website or directory.
7. The utility asks you to choose an ID for the package. Accept the default ID or type a different one.
8. The utility asks you if authentication is needed to access the package. If it is, type “Yes” and type the username and password when prompted. Otherwise, type “No”.
9. The utility asks you where you want to store the cached package files. Accept the default directory or type a different one.
10. The utility asks you if you want to enter details for another package. Unless you customize your Linux kernels, you should only need one package per update group. Type “No”.
11. When you have finished entering package details, the utility asks you if any computers that will be part of this update group will themselves act as update servers for other computers. Type “Yes” or “No” as appropriate. The utility finishes adding the update group to the offline corporate configuration file.
12. Run the utility `addcfg` to copy the configuration to the central installation directory, ready for workstations to download when they next update. The utility is in the CID. Depending on where the CID is, type

```
/opt/sophos-av/update/cache/LOCAL/PACKAGE/addcfg.sh -fCONFIG-FILE
```

where CONFIG-FILE is the path of the offline corporate configuration file.

Now assign computers to this update group ([section 15.2.4](#)).

### 15.2.3 Configuring an existing update group

Details of the update groups are stored in the corporate configuration file. (For more information about this file, refer to [section 7.3](#).) To configure an existing update group in the corporate configuration file, go to the computer where you created the corporate configuration file. You can set the individual update parameters of an update group using the utility `savconfig`. (For more information about this utility, refer to [section 7.1](#).) You must update the offline corporate configuration file, and then use the utility `addcfg` to apply the changes to the live corporate configuration file.

When you set a parameter, you must specify the update group and the package as well as the parameter itself, unless you are setting the frequency of updating. The following examples assume the group is GRP-A and the package is PCKG1. You must also specify the path of the offline corporate configuration file (represented here by CONFIG-FILE) and that you are accessing the corporate layer of this file.

To set the location of the update source, use the parameter UpdateSourcePath. For example, type

```
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c set UpdateSourcePath
GRP-A PCKG1 PATH
```

where PATH is the location.

If you need a username and password to access the update source, use the parameters UpdateSourceUsername and UpdateSourcePassword, respectively. For example, type

```
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c set
UpdateSourceUsername GRP-A PCKG1 admin1
```

To set the location of the update cache, use the parameter UpdateCachePath. For example, type

```
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c set UpdateCachePath
GRP-A PCKG1 PATH
```

where PATH is the location.

If computers in this update group are going to act as update servers for other computers, set the parameter UpdateVendors to the Linux distributions that need to be updated. Currently, valid values are turbo, suse, debian and redhat. For example, if this computer is going to provide updates for computers running SUSE or Debian, type

```
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c UpdateVendors GRP-A
PCKG1 suse debian
```

To set how often Sophos Anti-Virus updates itself, use the parameter UpdatePeriod and specify the interval in hours. The frequency applies to the whole update group, so you don't need to specify which package. For example, type

```
/opt/sophos-av/bin/savconfig -f CONFIG-FILE -c set UpdatePeriod
GRP-A 2
```

Remember to use the utility addcfg to apply the changes to the live corporate configuration file.


Now assign computers to this update group (section 15.2.4).

### 15.2.4 Assigning a computer to the update group

1. At the computer that you want to assign, run the utility `savsetup`, which is in the `bin` subdirectory of the installation:

```
/opt/sophos-av/bin/savsetup
```

2. The utility asks you to select what you want to do. Select **Updating configuration**.
3. The utility asks you to select what you want to do. Select **Select update group for this computer**.
4. The utility displays the update groups that have been set up. Type the group that you want this computer to use. The utility assigns the computer to that update group.

-  If the update group that you want to use is not displayed, it might be because this computer has not got the latest corporate configuration. Try updating Sophos Anti-Virus immediately, as described in [section 13](#).

## 15.3 Configuring updating for a single computer

You can configure a computer that is not part of a network to update directly from Sophos, if it has an internet connection. You can check the current updating configuration ([section 15.3.1](#)). Then, configure the computer ([section 15.3.2](#)).

### 15.3.1 Checking the updating configuration for the computer

1. At the computer, run the utility `savsetup`, which is in the `bin` subdirectory of the installation.

```
/opt/sophos-av/bin/savsetup
```

2. The utility asks you to select what you want to do. Select **Updating configuration**.
3. The utility asks you to select what you want to do. Select **Display update configuration** to see the current configuration.

### 15.3.2 Configuring the computer to update from Sophos

You can configure the computer to update using either

- the utility `savsetup`, which is easier to use but limited, or
- the command `savconfig`, which enables you to set any parameter.

#### **savsetup**

1. At the computer, run the utility `savsetup`, which is in the `bin` subdirectory of the installation:

```
/opt/sophos-av/bin/savsetup
```

2. The utility asks you to select what you want to do. Select **Updating configuration**.
3. The utility asks you to select what you want to do. Select **Configure computer to update from Sophos**.
4. The utility asks you for the username for the updates. Type the username that Sophos gave you.
5. The utility asks you for the password for the updates. Type the password that Sophos gave you. The utility configures the computer to update from Sophos.

#### **savconfig**

You can set the individual update parameters using the utility `savconfig`. (For more information about this utility, refer to [section 7.1](#).) When you set a parameter, you must specify the update group and the package as well as the parameter itself, unless you are setting the frequency of updating.

To set the update group, use the parameter `UpdateGroup`. For example, type

```
/opt/sophos-av/bin/savconfig set UpdateGroup LOCAL
```

To set the package from which that update group should update, use the parameter `UpdateFromPackage`. For example, type

```
/opt/sophos-av/bin/savconfig set UpdateFromPackage LOCAL PACKAGE
```

To set the location of the update source to be Sophos, use the parameter `UpdateSourcePath` and the value `"sophos:"`. For example, type

```
/opt/sophos-av/bin/savconfig set UpdateSourcePath LOCAL PACKAGE
sophos:
```

To set the username and password needed to access the update source, use the parameters `UpdateSourceUsername` and `UpdateSourcePassword`, respectively. For example, type

```
/opt/sophos-av/bin/savconfig set UpdateSourceUsername LOCAL PACKAGE  
admin1
```

To set the location of the update cache, use the parameter `UpdateCachePath`. For example, type

```
/opt/sophos-av/bin/savconfig set UpdateCachePath LOCAL PACKAGE PATH
```

where `PATH` is the location.

To set how often Sophos Anti-Virus updates itself, use the parameter `UpdatePeriod` and specify the interval in hours. You don't need to specify the package. For example, type

```
/opt/sophos-av/bin/savconfig set UpdatePeriod LOCAL 2
```

## ***Troubleshooting***

## 16 Troubleshooting

This section provides answers to some common problems that you may encounter when using Sophos Anti-Virus. (For more information about Sophos Anti-Virus error codes for on-demand scans, refer to [section 3.6](#).)

If your problem is not described in this section, refer to the Sophos website [www.sophos.com](http://www.sophos.com) which includes a support knowledgebase, virus analyses, the latest IDEs, product downloads and technical articles.

If your problem is not described on the website, contact Sophos [technical support](#).

### 16.1 Unable to run a command

If you are unable to run a command, it might be because you don't have sufficient privileges. Try logging in with root privileges.

### 16.2 Exclusion configuration hasn't been applied

Occasionally, when you configure Sophos Anti-Virus to include items for scanning that were previously excluded, the items remain excluded. Try flushing the cache of files that have previously been scanned:

```
echo 'disable' > /proc/sys/talpa/intercept-filters/Cache/status
echo 'enable' > /proc/sys/talpa/intercept-filters/Cache/status
```

### 16.3 man page not found

If the system returns this message when you try to view a Sophos Anti-Virus man page, you probably need to change your system settings. Ensure that the environment variable MANPATH in your login script or profile includes /usr/local/man. If it does not include this path, add it to the environment variable as shown in the examples below. Do not alter any of the existing settings.

**If you are running the sh, ksh or bash shell, enter**

```
MANPATH=$MANPATH:/usr/local/man
export MANPATH
```

**If you are running the csh or tsh shell, enter**

```
setenv MANPATH [values]:/usr/local/man
```

where [values] are the existing settings.

You should make these variables system-wide. To do this, amend `/etc/login` or `/etc/profile`.

- ❗ If you **do not** have a login script, you will need to reset these values every time you restart the computer.

## 16.4 Sophos Anti-Virus runs out of disk space

This problem may arise when scanning complex archive files.

When it unpacks archive files, Sophos Anti-Virus uses the `/tmp` directory to store its working results. If this directory is not very large, Sophos Anti-Virus may run out of disk space. Specific users may encounter the same problem if Sophos Anti-Virus exceeds their quota.

The solution is to enlarge `/tmp` or increase the users' quota. Alternatively, change the directory Sophos Anti-Virus uses for working results. You can do this by setting the environment variable `SAV_TMP`.

## 16.5 On-demand scanning runs slowly

### Full scan

By default, Sophos Anti-Virus performs a quick scan, which scans only the parts of files likely to contain viruses. However, if scanning is set to full, it scans everything, and takes significantly longer to carry out a scan.

See the `-f` [qualifier](#) in section 9.6.1.

- ❗ **Full scanning is needed in order to detect some viruses, but should only be enabled on a case-by-case basis (e.g. on advice from Sophos technical support).**

### Scanning all files

By default, Sophos Anti-Virus checks only files defined as executables. If it is configured to check all files the process takes longer. If you would like to scan other specific extensions, as well as executable files, add those extensions to the list of extensions Sophos Anti-Virus defines as executables.

See the `-all` and `-ext=` [qualifiers](#) in section 9.6.1.

## 16.6 Archiver backs up all files that have been scanned on demand

Your archiver may always back up all the files that Sophos Anti-Virus has scanned on demand. This can happen due to changes that Sophos Anti-Virus makes in the 'status-changed' time of files.

By default, Sophos Anti-Virus attempts to reset the access time (atime) of files to the time shown before scanning. However, this has the effect of changing the inode status-changed time (ctime). If your archiver uses the ctime to decide whether a file has changed, it backs up all files scanned by Sophos Anti-Virus.

To prevent such backups, run the savscan command with the --no-reset-atime qualifier.

## 16.7 Virus not cleaned up

If Sophos Anti-Virus has not attempted to clean up a virus, check that automatic cleanup has been enabled.

If Sophos Anti-Virus could not disinfect the virus ('Disinfection failed'), it may be that it cannot disinfect that type of virus.

You should also check the following:

- If dealing with a removable medium (e.g. floppy disk, CD), make sure that it is not write-protected.
- If dealing with files on an NTFS filesystem, make sure that it is not write-protected.

Sophos Anti-Virus does not disinfect a virus fragment because it has not found an exact virus match. Refer to section 16.8.

## 16.8 Virus fragment reported

If a virus fragment is reported, contact Sophos [technical support](#) for advice.

The report of a virus fragment indicates that part of a file matches part of a virus. There are three possible causes:

### **Variant of a known virus**

Many new viruses are based on existing ones, so that code fragments typical of a known virus may appear in files infected with a new one. If a virus fragment is reported, it is possible that Sophos Anti-Virus has detected a new virus, which could become active.

### **Corrupted virus**

Many viruses contain bugs in their replication routines that cause them to infect target files incorrectly. An inactive portion of the virus (possibly a substantial part) may appear within the host file, and this is detected by Sophos Anti-Virus. A corrupted virus cannot spread.

### **Database containing a virus**

When running a full scan, Sophos Anti-Virus may report that there is a virus fragment in a database file.

## **16.9 “Connection refused” error when accessing the GUI**

When you try to access the Sophos Anti-Virus GUI, if an error message is displayed that tells you that the connection was refused, it might be because the Sophos Anti-Virus GUI daemon is not running. To start it, type

```
/etc/init.d/sav-web start
```

## **16.10 SUSE 8.0 computers don't get updated**

If you find that Sophos Anti-Virus is not being updated on computers that are running SUSE 8.0, modify the update group to which they belong. To do this, do as follows:

1. Go to the update server that provides updates for the SUSE 8.0 computers.
2. Configure the update group as explained in [section 15.2.3](#). Change the value of the UpdateVendors parameter by adding “turbo” to the list of Linux distributions.

When the update server is itself updated, it should have the correct updates ready for the SUSE 8.0 computers to download.



## ***Appendix***

**Locales**

## Appendix 1 Locales

The following is a list of the locales that are used by alerting and logging. Each language has a non-region-specific locale (e.g. “en”) and region-specific locales (e.g. “en\_GB”). The non-region-specific locale can be used when you want to address people in different regions who speak a similar language.

<b>Language</b>	<b>Locale</b>
Albanian	sq
Albanian (Albania)	sq_AL
Arabic	ar
Arabic (Arabic countries)	ar_AA
Arabic (Bahrain)	ar_BH
Arabic (Egypt)	ar_EG
Arabic (Jordan)	ar_JO
Arabic (Kuwait)	ar_KW
Arabic (Lebanon)	ar_LB
Arabic (Oman)	ar_OM
Arabic (Qatar)	ar_QA
Arabic (Saudi Arabia)	ar_SA
Arabic (Syria)	ar_SY
Arabic (Tunisia)	ar_TN
Arabic (United Arab Emirates)	ar_AE
Bulgarian	bg
Byelorussian	be
Byelorussian (Belarus)	be_BY
Catalan	ca
Catalan (Spain)	ca_ES
Chinese	zh
Chinese Simplified (People’s Republic of China)	zh_CN
Chinese Traditional (Republic of China)	zh_TW
Croatian	hr
Croatian (Croatia)	hr_HR
Czech	cs
Czech (Czech Republic)	cs_CZ
Danish	da
Danish (Denmark)	da_DK
Dutch	nl
Dutch (Belgium)	nl_BE
Dutch (Netherlands)	nl_NL
English	en
English (Australia)	en_AU
English (Belgium)	en_BE

<b>Language</b>	<b>Locale</b>
English (Canada)	en_CA
English (Great Britain)	en_GB
English (India)	en_IN
English (Ireland)	en_IE
English (New Zealand)	en_NZ
English (South Africa)	en_ZA
English (United States)	en_US
Estonian	ET
Estonian (Estonia)	ET_EE
Finnish	fi
Finnish (Finland)	fi_FI
French	fr
French (Belgium)	fr_BE
French (Canada)	fr_CA
French (France)	fr_FR
French (Luxembourg)	fr_LU
French (Switzerland)	fr_CH
German	de
German (Austria)	de_AT
German (Germany)	de_DE
German (Luxembourg)	de_LU
German (Switzerland)	de_CH
Greek	el
Greek (Greece)	el_GR
Hebrew	iw
Hebrew (Israel)	iw_IL
Hindi	hi
Hindi (India)	hi_IN
Hungarian	hu
Hungarian (Hungary)	hu_HU
Icelandic	is
Icelandic (Iceland)	is_IS
Italian	it
Italian (Italy)	it_IT
Italian (Switzerland)	it_CH
Japanese	ja
Japanese (Japan)	ja_JP
Korean	ko
Korean (Korea)	ko_KR
Latvian	lv
Latvian (Latvia)	lv_LV
Lithuanian	lt
Lithuanian (Lithuania)	lt_LT

<b>Language</b>	<b>Locale</b>
Macedonian	mk
Macedonian (Former Yugoslav Republic of Macedonia)	mk_MK
Norwegian	no
Norwegian (Norway)	no_NO
Polish	pl
Polish (Poland)	pl_PL
Portuguese	pt
Portuguese (Brazil)	pt_BR
Portuguese (Portugal)	pt_PT
Romanian	ro
Romanian (Romania)	ro_RO
Russian	ru
Russian (Russia)	ru_RU
Serbian (Cyrillic)	sr
Serbian (Cyrillic) (Yugoslavia)	sr_SP
Serbian (Cyrillic) (Yugoslavia)	sr_YU
Serbian (Latin)	sh
Serbian (Latin) (Yugoslavia)	sh_SP
Serbian (Latin) (Yugoslavia)	sh_YU
Slovak	sk
Slovak (Slovakia)	sk_SK
Slovene	sl
Slovene (Slovenia)	sl_SI
Spanish	es
Spanish (Argentina)	es_AR
Spanish (Chile)	es_CL
Spanish (Columbia)	es_CO
Spanish (Mexico)	es_MX
Spanish (Peru)	es_PE
Spanish (Puerto Rico)	es_PR
Spanish (Spain)	es_ES
Spanish (Uruguay)	es_UY
Spanish (Venezuela)	es_VE
Swedish	sv
Swedish (Sweden)	sv_SE
Thai	th
Thai (Thailand)	th_TH
Turkish	tr
Turkish (Turkey)	tr_TR
Ukrainian	Uk
Ukrainian (Ukraine)	Uk_UA
Vietnamese	vi
Vietnamese (Vietnam)	vi_VN

## ***Glossary and index***

## Glossary

<b>Boot sector:</b>	The first part of the operating system to be read into memory when a computer is switched on (booted). The program stored in the boot sector is then executed, which loads the rest of the operating system from the system files on disk.
<b>Boot sector virus:</b>	A type of virus that subverts the initial stages of the booting process. A boot sector virus attacks either the master boot sector or the DOS boot sector.
<b>Central installation directory:</b>	Refer to CID.
<b>Corporate configuration file:</b>	Located in the CID. Stores Sophos Anti-Virus configuration that is to be applied across a network. Usually, changes are made to an offline file that is located elsewhere, and then these changes are applied to the live file in the CID using a utility.
<b>CID:</b>	Central installation directory; a central location on a network from which Sophos Anti-Virus is installed and updated. You must install a different CID for each platform, and make sure every CID is kept up to date.
<b>Cleanup:</b>	Cleanup is a general term that includes disinfection and deletion.
<b>Daemon:</b>	A process that runs in the background (i.e. independently of any user) with no input from or output to a terminal.
<b>Disinfection:</b>	Disinfection removes a virus from a file or boot sector. However, it doesn't undo any actions the virus has already taken.
<b>Executables:</b>	By default, when Sophos Anti-Virus performs an on-demand scan, it scans only files it defines as executables (even when full scanning is enabled). It is possible to: configure Sophos Anti-Virus to scan all files; to change the list of files defined as

executables; and to configure Sophos Anti-Virus to scan all files that *Linux* defines as executables. Refer to sections [9.6.1](#) and [9.6.2](#).

- Full scan:** If configured to perform full on-demand scanning, Sophos Anti-Virus scans all files and all parts of files in the area it has been configured to scan. A full scan takes significantly longer than a quick scan. It is occasionally necessary in order to locate certain viruses. Refer to [section 9.6.1](#).
- Local configuration file:** Located on a workstation. Stores Sophos Anti-Virus configuration that applies to that workstation.
- Macro virus:** A type of virus that uses macros in a data file to become active in memory and attach itself to other data files. Unlike other types of virus, macro viruses can attain a degree of platform independence.
- Master boot sector:** The first physical sector on the hard disk (sector 1, head 0, track 0) which is loaded and executed when the computer is switched on (booted). It contains the partition table as well as the code to load and execute the boot sector of the 'active' partition.
- Mount point:** The point on a filesystem at which there is a transparent link to an item or items on another filesystem on the same computer. Refer also to Symbolic link.
- On-access scanning:** Intercepts files as they are accessed, and grants access to only those that are virus free.
- On-demand scan:** A virus scan of the computer, or parts of the computer, that you can run immediately or schedule to run at another time.
- Quick scan:** The default on-demand scan type. Sophos Anti-Virus scans only the parts of files that can potentially contain executable code.
- Remote mount point:** The point on a filesystem at which there is a transparent link to an item or items on another

filesystem on a remote computer. Refer also to Symbolic link.

**Sophos Anti-Virus daemon:** Controls on-access scanning, and performs logging and alerting for on-access and on-demand scanning.

**Symbolic link:** A link to a file or directory on another filesystem or another computer.

**Syslog:** A facility that logs system messages (e.g. messages from a daemon). Refer also to Daemon.

**Trojan horse:** A computer program which carries out hidden and harmful functions. Generally Trojan horses trick the user into running them by claiming to have legitimate functionality. Backdoor Trojans enable other users to take control of your computer over the internet.

**Virus:** A computer program that can spread across computers and networks by attaching itself to a program (such as a macro or boot sector) and making copies of itself.

**Worm:** A type of virus that doesn't need a carrier program in order to replicate. Worms replicate themselves then use communications between computers (e.g. email programs) to spread.

# Index

## A

- alert
  - command-line 17, 59
  - desktop pop-up 17, 57
  - email 61
- archive
  - on-access scanning 44
  - multi-volume archive 35
  - on-demand scanning 47, 49

## B

- backtracking
  - preserving information 53
  - preventing 53
- backups of scanned files 83
- boot sector
  - on-access scanning 31
  - on-demand scanning 15

## C

- caching of scanned files 45
- CD boot image 55
- cleanup
  - getting information 18
  - on-access scanning 18
  - on-demand scanning 19, 49, 51
- command line
  - overview 8
  - reading arguments from file 53
- compressed file 52
- computer, scanning 14
- configuring across a network 27
- configuring on a single computer 30
- corrupt file 33

## D

- directory or file, scanning 14
- disinfection. See cleanup
- disk space insufficient 83

## E

- encrypted file 34
- error codes 15, 50
- excluding items, on-access scanning
  - file or directory 37
  - filesystem
    - from boot sector scanning 42
    - from file scanning 41
- excluding items, on-demand scanning
  - file, directory or filesystem 50

- executables
  - UNIX 53
  - Windows/DOS 50

## F

- file types, all 47
- filesystem, scanning 14
- full scan 50

## G

- GUI
  - configuring 69
  - connection problem 85
  - overview 8

## K

- kernel, customized 73
- kernel, new release 73

## L

- layer, in configuration 30
- log
  - Sophos Anti-Virus
    - configuring 68
    - viewing 23

## M

- magic number files 41
- mailbox 51
- man page not found 82
- MIME file 51

## Q

- quarantine 21, 54

## R

- recursive scanning 51
- remote computers, scanning 48

## S

- savconfig, overview 26
- savsetup, overview 27
- scheduling scanning 15
- screen output, copy to file/device 51
- slow on-demand scan 83
- special objects 55
- starting filesystem only, scanning 48
- starting on-access scanning 12
  - automatically on system boot 11
  - what is scanned when it is started 31

- status of on-access scanning 11
- stopping on-access scanning 13
  - what is scanned when it is stopped 31
- symbolically linked items 48, 53

## **U**

- updating
  - configuring 74
  - immediate 72
  - kernel, customized 73
  - kernel, new release 73

## **V**

- virus
  - analysis 18
  - fragment reported 84
  - not cleaned up 84
  - side-effects 22
- virus data
  - specifying location 51
- virus found
  - on-access scanning 17
  - on-demand scanning 17

## **Z**

- zip bomb 52

## Technical support

For technical support, visit

[www.sophos.com/support](http://www.sophos.com/support)

If you contact technical support, provide as much information as possible, including Sophos software version number(s), operating system(s) and patch level(s), and the exact text of any error messages.

Copyright 2005, 2006 Sophos Group. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

### **libmagic - file type detection**

Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others; maintained 1994-2004 Christos Zoulas.

This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at the beginning of the file, without modification, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### **Python**

#### **PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2**

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003, 2004 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.
4. PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

### **Medusa web server**

Medusa was once distributed under a 'free for non-commercial use' license, but in May of 2000 Sam Rushing changed the license to be identical to the standard Python license at the time. The standard Python license has always applied to the core components of Medusa, this change just frees up the rest of the system, including the http server, ftp server, utilities, etc. Medusa is therefore under the following license:

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Sam Rushing not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SAM RUSHING DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL SAM RUSHING BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Sam would like to take this opportunity to thank all of the folks who supported Medusa over the years by purchasing commercial licenses.

## **pycrypto**

Distribute and use freely; there are no restrictions on further dissemination and usage except those imposed by the laws of your country of residence. This software is provided "as is" without warranty of fitness for use or suitability for any purpose, express or implied. Use at your own risk or not at all.

Incorporating the code into commercial products is permitted; you do not have to make source available or contribute your changes back (though that would be nice).

--amk ([www.amk.ca](http://www.amk.ca))

## **OpenSSL cryptographic toolkit**

Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:  
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)).  
This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

### **TinyXml Xml parser**

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

### **Zlib compression tools**

(C) 1995-2002 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly      Mark Adler  
jloup@gzip.org      madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate \*not\* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.