SOPHOS

Sophos Anti-Virus for UNIX
user manual

Product version: 7
Document date: January 2011

Contents

1 About this manual....3
2 About Sophos Anti-Virus for UNIX....4
3 On-demand scanning....6
4 What happens if viruses are detected....10
5 Cleaning up viruses....11
6 View the Sophos Anti-Virus log....14
7 Update Sophos Anti-Virus immediately....15
8 Appendix A: On-demand scan return codes....16
9 Appendix B: About CID-based configuration....18
10 Appendix C: Configuring scheduled scans....23
11 Appendix D: Configuring email alerts....27
12 Appendix E: Configure logging....29
13 Appendix F: Configuring updating....30
14 Troubleshooting....33
15 Glossary....37
16 Technical support....38
17 Legal notices....39

1 About this manual

This manual tells you how to use and configure Sophos Anti-Virus for UNIX.

The manual assumes that you install and update Sophos Anti-Virus from a shared folder created by Sophos Enterprise Console.

To *install* Sophos Anti-Virus, see the *Sophos Endpoint Security and Control startup guide for Linux, NetWare, and UNIX*.

Sophos documentation is published at *www.sophos.com/support/docs/*.

2 About Sophos Anti-Virus for UNIX

2.1 What Sophos Anti-Virus does

Sophos Anti-Virus detects and deals with viruses (including worms and Trojans) on your UNIX computer. As well as being able to detect all UNIX viruses, it can also detect all non-UNIX viruses that might be stored on your UNIX computer and transferred to non-UNIX computers. It does this by scanning your computer.

2.2 How Sophos Anti-Virus protects your computer

Sophos Anti-Virus enables you to run an *on-demand scan*. An on-demand scan is a scan that you initiate. You can scan anything from a single file to everything on your computer that you have permission to read. You can either manually run an on-demand scan or schedule it to run unattended.

2.3 How you use Sophos Anti-Virus

Sophos Anti-Virus has a command-line interface. This enables you to access all the Sophos Anti-Virus functionality and to perform all configuration.

Note: You must be logged on to the computer as root to use all commands except **savscan**, which is used to run on-demand scans.

This manual assumes that you have installed Sophos Anti-Virus in the default location, /opt/sophos-av. The paths of the commands described are based on this location.

2.4 How you configure Sophos Anti-Virus

If your UNIX computers are managed by Sophos Enterprise Console, configure Sophos Anti-Virus as follows:

- Configure **scheduled scans, alerting, logging, and updating** centrally from Enterprise Console. For information, see the Enterprise Console Help.

  Note: These features also include some parameters that cannot be set using Enterprise Console. You can set these parameters from the Sophos Anti-Virus command-line interface on each UNIX computer locally. Enterprise Console ignores them.

- Configure **on-demand scans** from the Sophos Anti-Virus command-line interface on each UNIX computer locally.

If you have a network of UNIX computers that is *not* managed by Enterprise Console, configure Sophos Anti-Virus as follows:

- Configure **scheduled scans, alerting, logging, and updating** centrally by editing a configuration file in the central installation directory (CID) from which the computers update. This is called CID-based configuration.
- Configure **on-demand scans** from the Sophos Anti-Virus command-line interface on each computer locally.

Note: Do not use CID-based configuration unless technical support advises you to do so, or you cannot use Enterprise Console. You cannot use Enterprise Console configuration and CID-based configuration together.

If you have a standalone UNIX computer that is *not* managed by Enterprise Console, configure all Sophos Anti-Virus functionality from the Sophos Anti-Virus command-line interface.

3 On-demand scanning

An *on-demand scan* is a scan that you initiate. You can scan anything from a single file to everything on your computer that you have permission to read. You can either manually run an on-demand scan or schedule it to run unattended.

To schedule an on-demand scan, see *Appendix C: Configuring scheduled scans* (page 23).

3.1 Running on-demand scans

The command that you type to run an on-demand scan is **savscan**.

3.1.1 Scan the computer

- To scan the computer, type:
  savscan /

Note: You can also use Sophos Enterprise Console to run a full scan on one or more computers. For details, see the Enterprise Console Help.

3.1.2 Scan a particular directory or file

- To scan a particular directory or file, specify the path of the item. For example, type:
  savscan /usr/mydirectory/myfile

  You can type more than one directory or file in the same command.

3.1.3 Scan a filesystem

- To scan a filesystem, specify its name. For example, type:
  savscan /home

  You can type more than one filesystem in the same command.

3.2 Configuring on-demand scans

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

To see a full list of the options that you can use with an on-demand scan, type:

man savscan

3.2.1 Scan all file types

By default, Sophos Anti-Virus scans only executables. To see a full list of the file types that Sophos Anti-Virus scans by default, type **savscan -vv**.

- To scan all file types, not just those that are scanned by default, use the option **-all**. Type:
  savscan *path* **-all**

  Note: This makes scanning take longer, can compromise performance on servers, and can cause false virus reports.

3.2.2 Scan a particular file type

By default, Sophos Anti-Virus scans only executables. To see a full list of the file types that Sophos Anti-Virus scans by default, type **savscan -vv**.

- To scan a particular file type, use the option **-ext** with the appropriate filename extension. For example, to scan files that have the filename extension .txt, type:
  savscan *path* **-ext=txt**
- To disable scanning of a particular file type, use the option **-next** with the appropriate filename extension.

Note: To specify more than one file type, separate each filename extension with a comma.

3.2.3 Scan inside all archive types

You can configure Sophos Anti-Virus to scan inside all archive types. To see a list of these archive types, type **savscan -vv**.

- To scan inside all archive types, use the option **-archive**. Type:
  savscan *path* **-archive**

  Archives that are "nested" within other archives (for example, a TAR archive within a ZIP archive) are scanned recursively.

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

3.2.4 Scan inside a particular archive type

You can configure Sophos Anti-Virus to scan inside a particular archive type. To see a list of these archive types, type **savscan -vv**.

- To scan inside a particular archive type, use the option that is shown in the list. For example, to scan inside TAR and ZIP archives, type:

savscan *path* **-tar -zip**

Archives that are "nested" within other archives (for example, a TAR archive within a ZIP archive) are scanned recursively.

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

3.2.5 Scan remote computers

By default, Sophos Anti-Virus does not scan items on remote computers (that is, does not traverse remote mount points).

- To scan remote computers, use the option **--no-stay-on-machine**. Type:
  savscan *path* **--no-stay-on-machine**

3.2.6 Turn off scanning of symbolically linked items

By default, Sophos Anti-Virus scans symbolically linked items.

- To turn off scanning of symbolically linked items, use the option **--no-follow-symlinks**. Type:
  savscan *path* **--no-follow-symlinks**

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

3.2.7 Scan the starting filesystem only

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

- To scan the starting filesystem only, use the option **--stay-on-filesystem**. Type:
  savscan *path* **--stay-on-filesystem**

3.2.8 Excluding items from scanning

You can configure Sophos Anti-Virus to exclude particular items (files, directories, or filesystems) from scanning by using the option **-exclude**. Sophos Anti-Virus excludes any items that follow the option in the command string. For example, to scan items fred and harry, but not tom or peter, type:

savscan fred harry -exclude tom peter

You can exclude directories or files that are *under* a particular directory. For example, to scan all of Fred's home directory, but exclude the directory games (and all directories and files under it), type:

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

You can also configure Sophos Anti-Virus to *include* particular items that follow the option **-include**. For example, to scan items fred, harry, and bill, but not tom or peter, type:

savscan fred harry -exclude tom peter -include bill

3.2.9 Scan file types that UNIX defines as executables

By default, Sophos Anti-Virus does not scan file types that UNIX defines as executables.

- To scan file types that UNIX defines as executables, use the option **--examine-x-bit**. Type: **savscan** *path* **--examine-x-bit**

  Sophos Anti-Virus still scans files that have filename extensions that are in its own list as well. To see a list of these filename extensions, type **savscan -vv**.

4 What happens if viruses are detected

If an on-demand scan detects a virus, by default Sophos Anti-Virus:

- Logs the event in syslog and the Sophos Anti-Virus log (see *View the Sophos Anti-Virus log* (page 14)).
- Sends an alert to Enterprise Console if it is being managed by Enterprise Console.
- Sends an email alert to root@localhost.
- Displays a command-line alert. It reports the virus on the line which starts with >>> followed by either `Virus` or `Virus Fragment`:

```
SAVScan virus detection utility
Version 4.50.0 [Linux/Intel]
Virus data version 4.50, February 2010
Includes detection for 1375239 viruses, Trojans and worms
Copyright (c) 1989-2010 Sophos Group. All rights reserved.

System time 13:43:32, System date 02 March 2010

IDE directory is: /opt/sophos-av/lib/sav

Using IDE file nyrate-d.ide
. . . . . .
Using IDE file injec-lz.ide

Quick Scanning

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

33 files scanned 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 or email support@sophos.com
End of Scan.
```

For information about cleaning up viruses, see *Cleaning up viruses* (page 11).

5 Cleaning up viruses

5.1 Get cleanup information

If viruses are reported, you can get information and cleanup advice from the Sophos website.

To get cleanup information:

1. Go to the security analyses page (*www.sophos.com/security/analyses*).
2. Search for the analysis of the virus, by using the name that was reported by Sophos Anti-Virus.

5.2 Quarantining infected files

You can configure an on-demand scan to put infected files into quarantine to prevent them from being accessed. It does this by changing the ownership and permissions for the files.

Note: If you specify disinfection (see *Cleaning up infected files* (page 12)) as well as quarantining, Sophos Anti-Virus attempts to disinfect infected items and quarantines them only if disinfection fails.

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

5.2.1 Specify quarantining

- To specify quarantining, use the option **--quarantine**. Type:
  savscan *path* **--quarantine**

5.2.2 Specifying the ownership and permissions that are applied

By default, Sophos Anti-Virus changes:

- The user ownership of an infected file to the user running Sophos Anti-Virus.
- The group ownership of the file to the group to which that user belongs.
- The file permissions to `-r--------` (0400).

If you prefer, you can change the user or group ownership and file permissions that Sophos Anti-Virus applies to infected files. You do so by using these parameters:

```
uid=nnn
user=username
gid=nnn
group=group-name
mode=ppp
```

You cannot specify more than one parameter for user ownership or for group ownership. For example, you cannot specify a **uid** *and* a **user**.

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

For example:

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

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

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

5.3 Cleaning up infected files

You can configure an on-demand scan to clean up (disinfect or delete) infected files. Any actions that Sophos Anti-Virus takes against infected files are listed in the scan summary and logged in the Sophos Anti-Virus log. By default, cleanup is disabled.

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

5.3.1 Disinfect a specific infected file

- To disinfect a specific infected file, use the option **-di**. Type:
  savscan *path* **-di**

  Sophos Anti-Virus asks for confirmation before it disinfects.

  Note: Disinfecting an infected document does not repair any changes the virus has made to the document. (See *Get cleanup information* (page 11) to find out how to view details on the Sophos website of the virus's side-effects.)

5.3.2 Disinfect all infected files on the computer

- To disinfect all infected files on the computer, type:
  savscan / -di

  Sophos Anti-Virus asks for confirmation before it disinfects.

  Note: Disinfecting an infected document does not repair any changes the virus has made to the document. (See *Get cleanup information* (page 11) to find out how to view details on the Sophos website of the virus's side-effects.)

5.3.3 Delete a specific infected file

- To delete a specific infected file, use the option **-remove**. Type:
  savscan *path* **-remove**

  Sophos Anti-Virus asks for confirmation before it deletes.

5.3.4 Delete all infected files on the computer

- To delete all infected files on the computer, type:
  savscan / -remove

  Sophos Anti-Virus asks for confirmation before it deletes.

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. If you did not have them before you were infected, start keeping 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: see *Technical support* (page 38).

6 View the Sophos Anti-Virus log

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.

- To view the Sophos Anti-Virus log, at a command prompt, use the command **savlog**. This can be used with various options to restrict the output to certain messages and to 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

7 Update Sophos Anti-Virus immediately

Provided that you have enabled auto-updating, Sophos Anti-Virus is kept updated automatically. However, you can also update Sophos Anti-Virus immediately, without waiting for the next automatic update.

- To update Sophos Anti-Virus immediately, at the computer that you want to update, type: **/opt/sophos-av/bin/savupdate**

Note: You can also update computers immediately from Sophos Enterprise Console.

8 Appendix A: On-demand scan return codes

savscan returns a code to the shell that indicates the result of the scan. You can view the code by entering a further command after the scan has finished, for example:

echo $?

Return code	Description
0	No errors occur and no viruses are detected
1	The user interrupts the scan by pressing CTRL+C
2	An error occurs that prevents further execution of a scan
3	A virus is detected

8.1 Extended return codes

savscan returns a more detailed code to the shell if you run it with the **-eec** option. You can view the code by entering a further command after the scan has finished, for example:

echo $?

Extended return code	Description
0	No errors occur and no viruses are detected
8	A survivable error occurs
16	A password-protected file is found (it is not scanned)
20	An item containing a virus is detected and disinfected
24	An item containing a virus is found and not disinfected
28	A virus is detected in memory
32	An integrity check failure occurs

Extended return code	Description
36	An unsurvivable error occurs
40	The scan is interrupted

9 Appendix B: About CID-based configuration

Central installation directory (CID)-based configuration is an alternative to configuration from Sophos Enterprise Console. You can use it to configure all features except on-demand scans, for which you should see *Configuring on-demand scans* (page 6).

Note: Do not use CID-based configuration unless technical support advises you to do so, or you cannot use Enterprise Console. You cannot use Enterprise Console configuration and CID-based configuration together.

CID-based configuration does not require a Windows computer. It involves making changes to a configuration file that is stored in the CID, by setting the values of parameters using the command **savconfig** (see *savconfig configuration command* (page 21)). Then, when computers update from the CID, they use this configuration.

You can also lock any parameters so that they cannot be modified on client computers. In this way, you can determine the configuration of Sophos Anti-Virus on each computer, without fear that the settings will be changed by the user of that computer.

There are two configuration files: the *live* configuration file in the CID and the *offline* configuration file stored elsewhere. When you want to change the live file, you change the offline file, and replace the live file with the offline file. This is explained in the following sections.

9.1 Create a CID-based configuration

1. Use the command **savconfig** to set the value of each parameter that you want to set in the offline configuration file.

   Use the following syntax:

   /opt/sophos-av/bin/savconfig -f *config-file* **-c** *operation parameter value*

   where:

   - **-f** specifies that the setting is to be applied to the offline file.
   - *config-file* is the path of the offline file, which can be in any directory other than the CID. **savconfig** creates the file for you.
   - **-c** indicates that you want to access the Corporate layer of the offline file (for more information about layers, see *About configuration layers* (page 21)).
   - *operation* is either **set**, **update**, **add**, **remove**, or **delete**.
   - *parameter* is the parameter that you want to set.
   - *value* is the value to which you want to set the parameter.

   For example, to create a file called CIDconfig.cfg in the directory ./config and to disable email alerts, type:

   /opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c set EmailNotifier Disabled

   For information about using **savconfig**, see *savconfig configuration command* (page 21).

2. To view the parameter values, use the **query** operation. You can view the value of an individual parameter or all parameters. For example, to view the values of all the parameters that you have set, type:
   /opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c query

3. When you have finished setting parameters, update Sophos Anti-Virus:
   /opt/sophos-av/bin/savupdate

4. Run the command **addcfg** with the option **-f** and the path of the offline configuration file:
   /opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f*config-file*

5. Copy the directory /opt/sophos-av/update/cache/Primary-unpacked/config to the CID.

   The new configuration is now available for computers to download the next time that they update.

9.2 Update a CID-based configuration

1. Use the command **savconfig** to set the value of each parameter that you want to set in the offline configuration file.

   Use the following syntax:

   /opt/sophos-av/bin/savconfig -f *config-file* **-c** *operation parameter value*

   where:

   - **-f** specifies that the setting is to be applied to the offline file.
   - *config-file* is the path of the offline file.
   - **-c** indicates that you want to access the Corporate layer of the offline file (for more information about layers, see *About configuration layers* (page 21)).
   - *operation* is either **set**, **update**, **add**, **remove**, or **delete**.
   - *parameter* is the parameter that you want to set.
   - *value* is the value to which you want to set the parameter.

   For example, to update a file called CIDconfig.cfg in the directory ./config and to disable email alerts, type:

   /opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c set EmailNotifier Disabled

   Note: You must set *all* the parameters that you want to retain in the Corporate layer of the live file, not just those that you want to update. To use a copy of the current live configuration file as the offline file, copy CorporateLayer.cfg to any directory other than the CID. CorporateLayer.cfg is in the directory config in the CID.

   For information about using **savconfig**, see *savconfig configuration command* (page 21).

2. To view the parameter values, use the **query** operation. You can view the value of an individual parameter or all parameters. For example, to view the values of all the parameters that you have set, type:
   /opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c query

3. When you have finished setting parameters, update Sophos Anti-Virus:
   /opt/sophos-av/bin/savupdate

4. Run the command **addcfg** with the option **-f** and the path of the offline configuration file:
   /opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f*config-file*

5. Copy the directory /opt/sophos-av/update/cache/Primary-unpacked/config to the CID.

   The new configuration is now available for computers to download the next time that they update.

9.3 About configuration layers

Each installation of Sophos Anti-Virus includes a local configuration file, which includes settings for all features of Sophos Anti-Virus apart from on-demand scans.

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 CID.
- 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 configuration file in the CID, the Corporate layer in the local file is replaced by that of the file in the CID.

9.4 savconfig configuration command

savconfig is the command that you use to configure all features of Sophos Anti-Virus apart from on-demand scanning. The path of the command is /opt/sophos-av/bin. Using the command to configure specific functions of Sophos Anti-Virus is explained in the remainder of this manual. The rest of this subsection explains the syntax.

The syntax of **savconfig** is:

savconfig [*option*] **...** [*operation*] [*parameter*] [*value*] **...**

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

man savconfig

9.4.1 *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 about layers, see *About configuration layers*

(page 21). By default, the command accesses the User layer. 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. 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

If you are using Enterprise Console, you can display just the values of the anti-virus policy parameters by using the option **--consoleav**. Type:

/opt/sophos-av/bin/savconfig --consoleav query

You can display just the values of the Enterprise Console update policy by using the option **--consoleupdate**. Type:

/opt/sophos-av/bin/savconfig --consoleupdate query

9.4.2 *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. The operations enable you to add values to a list or remove values from a list. For example, the **Email** parameter is a *list* of email recipients.

To display the values of parameters, use the operation **query**. For example, to display the value of the **EmailNotifier** parameter, type:

/opt/sophos-av/bin/savconfig query EmailNotifier

If you are using Enterprise Console, when **savconfig** returns values of parameters, those that conflict with the relevant Enterprise Console policy are clearly marked with the word "Conflict".

9.4.3 *parameter*

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

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

Some parameters require secondary parameters to be specified as well.

9.4.4 *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 quotation marks.

10 Appendix C: Configuring scheduled scans

Sophos Anti-Virus can store definitions of one or more scheduled scans.

Note: You can also use Enterprise Console or the command **crontab** to scan computers at set times. For details, see the Enterprise Console Help or *Sophos support knowledgebase article 12176*, respectively. Scheduled scans that have been added using Enterprise Console have names that are prefixed with "SEC:" and cannot be updated or removed except by using Enterprise Console.

10.1 Add a scheduled scan from a file

1. To use a template scan definition as a starting point, open /opt/sophos-av/doc/namedscan.example.en.

   To create a scan definition from scratch, open a new text file.

2. Define what to scan, when to scan it, and any other options, using only the parameters listed in the template.

   To schedule the scan, you must include at least one day and one time.

3. Save the file in a location of your choosing, being careful not to overwrite the template.
4. Add the scheduled scan to Sophos Anti-Virus using the command **savconfig** with the operation **add** and the parameter **NamedScans**. Specify the name of the scan and the path of the scan definition file.

   For example, to add the scan Daily, which is stored in /home/fred/DailyScan, type:

   /opt/sophos-av/bin/savconfig add NamedScans Daily /home/fred/DailyScan

10.2 Add a scheduled scan from standard input

1. Add the scheduled scan to Sophos Anti-Virus using the command **savconfig** with the operation **add** and the parameter **NamedScans**. Specify the name of the scan and use a hyphen to specify that the definition is to be read from standard input.

   For example, to add the scan Daily, type:

   /opt/sophos-av/bin/savconfig add NamedScans Daily -

   When you press ENTER, Sophos Anti-Virus waits for you to type the definition of the scheduled scan.

2. Define what to scan, when to scan it, and any other options, using only the parameters listed in the template scan definition: /opt/sophos-av/doc/namedscan.example.en. After typing each parameter and its value, press ENTER.

   To schedule the scan, you must include at least one day and one time.

3. To complete the definition, press CTRL+D.

10.3 Export a scheduled scan to a file

- To export a scheduled scan from Sophos Anti-Virus to a file, use the command **savconfig** with the operation **query** and the parameter **NamedScans**. Specify the name of the scan and the path of the file to which you want to export the scan.

  For example, to export the scan Daily to the file /home/fred/DailyScan, type:

  /opt/sophos-av/bin/savconfig query NamedScans Daily > /home/fred/DailyScan

10.4 Export names of all scheduled scans to a file

- To export the names of all scheduled scans (including those that have been created usingEnterprise Console) from Sophos Anti-Virus to a file, use the command**savconfig** with the operation **query** and the parameter**NamedScans**. Specify the path of the file to which you want to export the scan names.

  For example, to export the names of all scheduled scans to the file/home/fred/AllScans, type:

  /opt/sophos-av/bin/savconfig query NamedScans > /home/fred/AllScans

  Note: `SEC:FullSystemScan` is a scan that is always defined if the computer is managed by Enterprise Console.

10.5 Export a scheduled scan to standard output

- To export a scheduled scan from Sophos Anti-Virus to standard output, use the command **savconfig** with the operation **query** and the parameter **NamedScans**. Specify the name of the scan.

  For example, to export the scan Daily to standard output, type:

  /opt/sophos-av/bin/savconfig query NamedScans Daily

10.6 Export names of all scheduled scans to standard output

- To export the names of all scheduled scans (including those that have been created usingEnterprise Console) from Sophos Anti-Virus to standard output, use the command **savconfig** with the operation **query** and the parameter **NamedScans**.

  For example, to export the names of all scheduled scans to standard output, type:

  /opt/sophos-av/bin/savconfig query NamedScans

  Note: `SEC:FullSystemScan` is a scan that is always defined if the computer is managed by Enterprise Console.

10.7 Update a scheduled scan from a file

Note: You cannot update scheduled scans that have been added using Enterprise Console.

1. Open the file that defines the scheduled scan that you want to update.

   If the scan is not already defined in a file, you can export the scan to a file, as explained in *Export a scheduled scan to a file* (page 24).

2. Amend the definition as necessary, using only the parameters listed in the template scan definition: /opt/sophos-av/doc/namedscan.example.en. You must define the scan completely, instead of just specifying what you want to update.
3. Save the file.
4. Update the scheduled scan in Sophos Anti-Virus using the command **savconfig** with the operation **update** and the parameter **NamedScans**. Specify the name of the scan and the path of the scan definition file.

   For example, to update the scan Daily, which is stored in /home/fred/DailyScan, type:

   /opt/sophos-av/bin/savconfig update NamedScans Daily /home/fred/DailyScan

10.8 Update a scheduled scan from standard input

Note: You cannot update scheduled scans that have been added using Enterprise Console.

1. Update the scheduled scan in Sophos Anti-Virus using the command **savconfig** with the operation **update** and the parameter **NamedScans**. Specify the name of the scan and use a hyphen to specify that the definition is to be read from standard input.

   For example, to update the scan Daily, type:

   /opt/sophos-av/bin/savconfig update NamedScans Daily -

   When you press ENTER, Sophos Anti-Virus waits for you to type the definition of the scheduled scan.

2. Define what to scan, when to scan it, and any other options, using only the parameters listed in the template scan definition: /opt/sophos-av/doc/namedscan.example.en. After typing each parameter and its value, press ENTER. You must define the scan completely, instead of just specifying what you want to update.

   To schedule the scan, you must include at least one day and one time.

3. To complete the definition, press CTRL+D.

10.9 Remove a scheduled scan

Note: You cannot remove scheduled scans that have been added using Enterprise Console.

- To remove a scheduled scan from Sophos Anti-Virus, use the command **savconfig** with the operation **remove** and the parameter **NamedScans**. Specify the name of the scan.

  For example, to remove the scan Daily, type:

  /opt/sophos-av/bin/savconfig remove NamedScans Daily

10.10 Remove all scheduled scans

Note: You cannot remove scheduled scans that have been added using Enterprise Console.

- To remove all scheduled scans from Sophos Anti-Virus, type:
  /opt/sophos-av/bin/savconfig delete NamedScans

11 Appendix D: Configuring email alerts

Note: If you are configuring a single computer that is on a network, the configuration might be overwritten if the computer downloads a new console-based or CID-based configuration.

You can configure Sophos Anti-Virus to send an email alert when it detects viruses, there is a scanning error, or some other type of error. Email alerts can be sent in English or Japanese.

11.1 Turn off email alerts

By default, email alerts are turned on.

- To turn off email alerts, type:
  /opt/sophos-av/bin/savconfig set EmailNotifier disabled

11.2 Specify the SMTP server hostname or IP address

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

- To specify the hostname or IP address of the SMTP server, use the parameter **EmailServer**. For example, type:
  /opt/sophos-av/bin/savconfig set EmailServer 171.17.31.184

11.3 Specify the language

By default, the language that is used for the alert message itself is English.

- To specify the language that is used for the alert message itself, use the parameter**EmailLanguage**. Currently, valid values are just "English" or "Japanese". For example, type:
  /opt/sophos-av/bin/savconfig set EmailLanguage Japanese

Note: This language selection applies only to the alert message itself, not the custom message that is included in each email alert in addition to the alert message itself.

11.4 Specify the email recipients

By default, Sophos Anti-Virus sends email alerts to root@localhost.

- To add an address to the list of recipients of email alerts, use the parameter**Email** with the operation **add**. For example, type:
  /opt/sophos-av/bin/savconfig add Email admin@localhost

  Note: You can specify more than one recipient in the same command. Separate each recipient by using a space.

- To remove an address from the list, use the parameter **Email** with the operation **remove**. For example, type:
  /opt/sophos-av/bin/savconfig remove Email admin@localhost

11.5 Turn on-demand email alerts off

By default, Sophos Anti-Virus emails the summary of an on-demand scan if, and only if, the scan detects viruses.

- To turn off the emailing of an on-demand scan summary if viruses are detected, type:
  /opt/sophos-av/bin/savconfig set EmailDemandSummaryIfThreat disabled

11.6 Specify what happens if an event is logged

By default, Sophos Anti-Virus sends an email alert when an event is logged in the Sophos Anti-Virus log. A custom English message is included in each alert in addition to the alert message itself. You can change the text of this custom message but it is not translated.

- To specify the custom message, use the parameter **LogMessage**. For example, type:
  /opt/sophos-av/bin/savconfig set LogMessage 'Contact IT'

12 Appendix E: Configure logging

Note: If you are configuring a single computer that is on a network, the configuration might be overwritten if the computer downloads a new console-based or CID-based configuration.

By default, scanning activity is logged in the Sophos Anti-Virus log: /opt/sophos-av/log/savd.log. When it reaches 1 MB in size, it is backed up to the same directory automatically and a new log is started.

- To see the default number of logs that are kept, type:
  /opt/sophos-av/bin/savconfig -s query LogMaxSizeMB
- To specify the maximum number of logs that are kept, use the parameter **LogMaxSizeMB**. For example, to set the maximum number of logs to 50, type:
  /opt/sophos-av/bin/savconfig set LogMaxSizeMB 50

13 Appendix F: Configuring updating

Important: If you manage Sophos Anti-Virus using Sophos Enterprise Console, you must configure updating using Enterprise Console. For information about how to do this, see the Enterprise Console Help instead of this section.

13.1 Basic concepts

Update server

An *update server* is a computer on which you have installed Sophos Anti-Virus and which also acts as an update source for other computers. These other computers are either update servers or update clients, depending on how you deploy Sophos Anti-Virus across the network.

Update client

An *update client* is a computer on which you have installed Sophos Anti-Virus and which does not need to act as an update source for other computers.

Primary update source

The *primary update source* is the location of the updates that a computer usually accesses. It might need access credentials.

Secondary update source

The *secondary update source* is the location of the updates that a computer accesses when the primary update source is unavailable. It might need access credentials.

13.2 savsetup configuration command

savsetup is a command that you can use to configure updating. You should use it only for the specific tasks explained in the following subsections.

Although it enables you to access only some of the parameters that you can access with **savconfig**, it is easier to use. It prompts you for values of parameters, and you respond by selecting or typing the values. To run **savsetup**, type:

/opt/sophos-av/bin/savsetup

13.3 Check the auto-updating configuration for a computer

1. At the computer that you want to check, type:
   /opt/sophos-av/bin/savsetup

   savsetup asks you to select what you want to do.

2. Select **Display update configuration** to see the current configuration.

13.4 Configure multiple update clients to update from the update server

Note: If you want to change the configuration for a single update client, see *Configure a single update client to update from the update server* (page 32) instead.

At the update server, you update the offline configuration file, and then apply the changes to the live configuration file, ready for the update clients to download the next time that they update. In the procedure below, *config-file* represents the path of the offline configuration file.

This section assumes that you want to configure the *primary* update source. However, if you want to configure the *secondary* update source, use the secondary update source parameters instead. For example, use **SecondaryUpdateSourcePath** instead of **PrimaryUpdateSourcePath**.

To configure multiple update clients to update from the update server:

1. Set the primary update source address to the location of the CID, using the parameter **PrimaryUpdateSourcePath**. You can specify either an HTTP address or a UNC path, depending on how you have set up the update server. For example, type:
   /opt/sophos-av/bin/savconfig -f *config-file* **-c set PrimaryUpdateSourcePath 'http://www.mywebcid.com/cid'**

2. If the primary update source requires authentication, set the username and password using the parameters **PrimaryUpdateUsername** and **PrimaryUpdatePassword**, respectively. For example, type:
   /opt/sophos-av/bin/savconfig -f *config-file* **-c set PrimaryUpdateUsername 'fred'**

   /opt/sophos-av/bin/savconfig -f *config-file* **-c set PrimaryUpdatePassword 'j23rjjfwj'**

3. If you access the primary update source via a proxy, set the address, username, and password of the proxy server, using the parameters **PrimaryUpdateProxyAddress**, **PrimaryUpdateProxyUsername**, and **PrimaryUpdateProxyPassword**, respectively. For example, type:
   /opt/sophos-av/bin/savconfig -f *config-file* **-c set PrimaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'**

   /opt/sophos-av/bin/savconfig -f *config-file* **-c set PrimaryUpdateProxyUsername 'penelope'**

   /opt/sophos-av/bin/savconfig -f *config-file* **-c set PrimaryUpdateProxyPassword 'fj202jrjf'**

4. When you have finished setting parameters, update Sophos Anti-Virus:
   /opt/sophos-av/bin/savupdate

5. Run the command **addcfg** with the option **-f** and the path of the offline configuration file:
   /opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f*config-file*

6. Copy the directory /opt/sophos-av/update/cache/Primary-unpacked/config to the CID.

   The new configuration is now available for computers to download the next time that they update.

13.5 Configure a single update client to update from the update server

Note: If you want to change the configuration for multiple update clients, see *Configure multiple update clients to update from the update server* (page 31) instead.

1. At the computer that you want to configure, type:
   /opt/sophos-av/bin/savsetup

   savsetup asks you to select what you want to do.

2. Select the option to configure the primary (or secondary) update source to be your own server.

   savsetup prompts you to enter details of the update source.

3. Enter the address of the source, and the username and password if required.
   You can specify either an HTTP address or a UNC path, depending on how you have set up the update server.

   savsetup asks you if you need a proxy to access the update server.

4. If you need a proxy, press Y and then type the proxy details.

14 Troubleshooting

This section describes how to deal with problems that might arise when usingSophos Anti-Virus.

For information about Sophos Anti-Virus return codes for on-demand scans, see *Appendix A: On-demand scan return codes* (page 16).

14.1 Unable to run a command

Symptom

Your computer does not allow you to run a Sophos Anti-Virus command.

Cause

This might be because you do not have sufficient privileges.

Resolve the problem

Try logging on to the computer as root.

14.2 Computer reports “No manual entry for ...”

Symptom

When you try to view a Sophos Anti-Virus man page, the computer displays a message similar to `No manual entry for ....`

Cause

This is probably because the environment variable MANPATH does not include the path to the man page.

Resolve the problem

1. If you are running the sh, ksh or bash shell, open /etc/profile for editing.

   If you are running the csh or tcsh shell, open /etc/login for editing.

   Note: If you do not have a login script or profile, carry out the following steps at the command prompt. You must do this every time that you restart the computer.

2. Check that the environment variable MANPATH includes the directory /usr/local/man.
3. If MANPATH does not include this directory, add it as follows. Do not change any of the existing settings.

   If you are running the sh, ksh or bash shell, type:

   MANPATH=$MANPATH:/usr/local/man

   export MANPATH

If you are running the csh or tcsh shell, type:

setenv MANPATH *values***:/usr/local/man**

where *values* are the existing settings.

4. Save the login script or profile.

14.3 Sophos Anti-Virus runs out of disk space

Symptom

Sophos Anti-Virus runs out of disk space, perhaps when scanning complex archives.

Causes

This might be for one of the following reasons:

- When it unpacks archives, 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.
- Sophos Anti-Virus has exceeded the user's quota.

Resolve the problem

Try one of the following:

- Enlarge /tmp.
- Increase the user's quota.
- Change the directory that Sophos Anti-Virus uses for working results. You can do this by setting the environment variable SAV_TMP.

14.4 On-demand scanning runs slowly

This problem may arise for one of the following reasons:

Symptom

Sophos Anti-Virus takes significantly longer to carry out an on-demand scan.

Causes

This might be for one of the following reasons:

- By default, Sophos Anti-Virus performs a quick scan, which scans only the parts of files that are likely to contain viruses. If scanning is set to full (using the option **-f**), it scans the whole file.
- By default, Sophos Anti-Virus scans only particular file types. If it is configured to scan *all* file types, the process takes longer.

Resolve the problem

Try one of the following, as appropriate:

- Avoid using full scanning unless you are advised to, for example by Sophos technical support.
- To scan files that have specific filename extensions, add those extensions to the list of file types that Sophos Anti-Virus scans by default. For more information, see *Scan a particular file type* (page 7).

14.5 Archiver backs up all files that have been scanned on demand

Symptom

Your archiver always backs up all the files that Sophos Anti-Virus has scanned on demand.

Cause

This is because of changes that Sophos Anti-Virus makes in the "status-changed" time of files. By default, Sophos Anti-Virus tries 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.

Resolve the problem

Run **savscan** with the option **--no-reset-atime**.

14.6 Virus not cleaned up

Symptoms

- Sophos Anti-Virus has not attempted to clean up a virus.
- Sophos Anti-Virus displays `Disinfection failed`.

Causes

This might be for one of the following reasons:

- Automatic cleanup has not been enabled.
- Sophos Anti-Virus cannot disinfect that type of virus.
- The infected file is on a removable medium, for example floppy disk or CD, that is write-protected.
- The infected file is on an NTFS filesystem.
- Sophos Anti-Virus does not clean up a virus fragment because it has not found an exact virus match.

Resolve the problem

Try one of the following, as appropriate:

- Enable automatic cleanup.
- If possible, make the removable medium writeable.
- Deal with files that are on an NTFS filesystem on the local computer instead.

14.7 Virus fragment reported

Symptom

Sophos Anti-Virus reports that it has detected a virus fragment.

Causes

This indicates that part of a file matches part of a virus. This is for one of the following reasons:

- Many new viruses are based on existing ones. Therefore, code fragments that are typical of a known virus might appear in files that are infected with a new one.
- Many viruses contain bugs in their replication routines that cause them to infect target files incorrectly. An inactive part of the virus (possibly a substantial part) may appear in the host file, and this is detected by Sophos Anti-Virus.
- When running a full scan, Sophos Anti-Virus may report that there is a virus fragment in a database file.

Resolve the problem

1. Update Sophos Anti-Virus on the affected computer so that it has the latest virus data.
2. Try to disinfect the file: see *Disinfect a specific infected file* (page 12).
3. If virus fragments are still reported, contact Sophos technical support for advice: see *Technical support* (page 38).

15 Glossary

central installation directory (CID)	A directory into which Sophos software and updates are placed. Networked computers update themselves from this directory.
CID	See "central installation directory".
CID-based configuration	Such configuration involves making changes to the CID-based configuration file by setting the values of parameters using the command **savconfig**. When computers update from the CID, they use this configuration. This method was formerly known as "corporate configuration".
disinfection	Disinfection removes a virus from a file or boot sector.
on-demand scan	A scan that you initiate. You can use an on-demand scan to scan anything from a single file to everything on your computer that you have permission to read.
primary update source	The location of the updates that a computer usually accesses. It might need access credentials.
scheduled scan	A scan of your computer, or parts of your computer, that runs at set times.
secondary update source	The location of the updates that a computer accesses when the primary update source is unavailable. It might need access credentials.
update client	A computer on which you have installed Sophos Anti-Virus and which does not need to act as an update source for other computers.
update server	A computer on which you have installed Sophos Anti-Virus and which also acts as an update source for other computers. These other computers are either update servers or update clients, depending on how you deploy Sophos Anti-Virus across the network.
virus	A computer program that copies itself. Often viruses disrupt computer systems or damage the data contained on them. A virus needs a host program and does not infect a computer until it has been run. Some viruses spread across networks by making copies of themselves or may forward themselves via email. The term "virus" is often also used to refer to viruses, worms, and Trojans.

16 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at *http://community.sophos.com/* and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at *http://www.sophos.com/support/*.
- Download the product documentation at *http://www.sophos.com/support/docs/*.
- Send an email to *support@sophos.com*, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

17 Legal notices

ACE™, TAO™, CIAO™, and CoSMIC™

techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledgethat any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, WashingtonUniversity, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me[21] know.

Douglas C. Schmidt[22]

References

1. http://www.cs.wustl.edu/~schmidt/ACE.html
2. http://www.cs.wustl.edu/~schmidt/TAO.html
3. http://www.dre.vanderbilt.edu/CIAO/
4. http://www.dre.vanderbilt.edu/cosmic/
5. http://www.dre.vanderbilt.edu/~schmidt/
6. http://www.cs.wustl.edu/~schmidt/ACE-members.html
7. http://www.wustl.edu/
8. http://www.uci.edu/
9. http://www.vanderbilt.edu/
10. mailto:doc_group@cs.wustl.edu
11. http://www.cs.wustl.edu/~schmidt/ACE-users.html
12. http://www.cs.wustl.edu/~schmidt/commercial-support.html
13. http://www.cs.wustl.edu/~schmidt/ACE.html
14. http://www.cs.wustl.edu/~schmidt/TAO.html
15. http://www.dre.vanderbilt.edu/CIAO/
16. http://www.dre.vanderbilt.edu/cosmic/
17. http://www.dre.vanderbilt.edu/
18. http://www.isis.vanderbilt.edu/
19. http://www.cs.wustl.edu/~schmidt/doc-center.html
20. http://www.opensource.org/
21. mailto:d.schmidt@vanderbilt.edu
22. http://www.dre.vanderbilt.edu/~schmidt/

GNU General Public License

Some software programs are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or similar Free Software licenses which, among other rights, permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires for any software licensed under the GPL, which is distributed to a user in an executable binary format, that the source code also be made available to those users. For any such software which is distributed along with this Sophos product, the source code is available by submitting a request to Sophos via email to *savlinuxgpl@sophos.com*. A copy of the GPL terms can be found at *www.gnu.org/copyleft/gpl.html*

libmagic – file type detection

Copyright © 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.

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998–2006 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.
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). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

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 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 acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

   The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "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.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

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)

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, worldwide 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 © 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 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.

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

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 jloup@gzip.org

Mark Adler 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.

Index

A

alerts
    command-line 10
    email 27
analyses of viruses 11
archives
    on-demand scans 7

B

backups of scanned files 35

C

CID-based configuration 4, 18
cleaning up infected files 12
cleanup information 11
CLI (command-line interface) 4
command-line alerts 10
command-line interface (CLI) 4
computer, on-demand scans 6
configuring Sophos Anti-Virus 4, 18

D

deleting infected files 13
directories, on-demand scans 6
disinfecting
    infected files 12
disk space insufficient 34

E

email alerts 27
Enterprise Console 4
error codes 16
excluding items
    on-demand scans 8

F

file types, on-demand scans 7, 9
files, on-demand scans 6
filesystems, on-demand scans 6, 8
fragment reported, viruses 36

I

infected files
    cleaning up 12
    deleting 13
    disinfecting 12
    quarantining 11

L

layers, in configuration file 21
log, Sophos Anti-Virus
    configuring 29
    viewing 14

M

man page not found 33

N

No manual entry for … 33

O

on-demand scans 6
    archives 7
    computer 6
    directories 6
    excluding items 8
    file types 7, 9
    files 6
    filesystems 6, 8
    remote computers 8
    scheduled scans 23
    symbolically linked items 8
    UNIX executables 9

Q

quarantining infected files 11

R

remote computers, on-demand scans 8
return codes 16

S

savconfig 21
savsetup 30
scheduled scans 23
side-effects of viruses 13
slow on-demand scans 34
Sophos Anti-Virus log
    configuring 29
Sophos Anti-Virus log *(continued)*
    viewing 14
symbolically linked items, on-demand scans 8

U

UNIX executables, on-demand scans 9
updating
    configuring 30
    immediate 15

V

viruses
    analyses 11
    detected 10, 28
    fragment reported 36
    not cleaned up 35
    side-effects 13