SOPHOS

Security made simple.

Sophos Anti-Virus for Linux configuration guide

Product version: 9

Document date: April 2016

Contents

1 About this guide

This guide tells you how to use and configure Sophos Anti-Virus for Linux.

You can find information on installation as follows:

To install Sophos Anti-Virus so that it can be managed with Sophos Cloud, log in to Sophos Cloud, go to the Downloads page and follow the instructions there.

To install Sophos Anti-Virus so that it can be managed with Sophos Enterprise Console, see the *Sophos Enterprise Console startup guide for Linux and UNIX*.

To install or uninstall unmanaged Sophos Anti-Virus on networked and single Linux computers, see the *Sophos Anti-Virus for Linux startup guide*.

Sophos documentation is published at http://www.sophos.com/en-us/support/documentation.aspx.

2 About Sophos Anti-Virus for Linux

2.1 What Sophos Anti-Virus does

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

2.2 How Sophos Anti-Virus protects your computer

On-access scanning is your main form of protection against viruses. Whenever you open, save or copy a file, Sophos Anti-Virus scans it and grants access to it only if it is safe.

Sophos Anti-Virus also enables you to run an on-demand scan to provide additional protection. 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

You perform all tasks by using the command-line interface.

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 document 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

The methods you use to configure Sophos Anti-Virus depend on whether you use Sophos management software (Sophos Enterprise Console or Sophos Cloud) or not.

Computers managed by Enterprise Console or Sophos Cloud

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

- Configure **on-access scanning, scheduled scans, alerting, logging, and updating** centrally from your management console. For information, see the Help in the management console.

  Note: These features also include some parameters that cannot be set centrally from the management console. You can set these parameters from the Sophos Anti-Virus CLI on each Linux computer locally. The management console ignores them.

- Configure **on-demand scans** from the Sophos Anti-Virus CLI on each Linux computer locally.

Networked computers not managed by Enterprise Console or Sophos Cloud

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

- Configure **on-access scanning, scheduled scans, alerting, logging, and updating** centrally by editing a configuration file from which the computers update. See Appendix: Extra Files configuration (page 24).
- Configure **on-demand scans** from the Sophos Anti-Virus CLI on each computer locally.

Note: Do not use Extra Files configuration unless technical support advises you to do so, or you cannot use a Sophos management console. You cannot use management console configuration and Extra Files configuration together.

Standalone computer not managed by Enterprise Console or Sophos Cloud

If you have a standalone Linux computer that is *not* managed by Enterprise Console or Sophos Cloud , configure all Sophos Anti-Virus functions from the CLI.

3 On-access scanning

On-access scanning is your main form of protection against viruses. Whenever you open, save or copy a file, Sophos Anti-Virus scans it and grants access to it only if it is safe.

3.1 Check that on-access scanning is active

- To check that on-access scanning is active, type:
  `/opt/sophos-av/bin/savdstatus`

3.2 Check that on-access scanning will be started automatically on boot

To perform this procedure, you must be logged on to the computer as root.

1. Check that **`savd`** will be started automatically on system boot:
   `chkconfig --list`

   Note: If this command does not work on your Linux distribution, use the appropriate utility to display services that are configured to start on system boot.

   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, type:

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

2. Check that on-access scanning will be started automatically with **`savd`**:
   `/opt/sophos-av/bin/savconfig query EnableOnStart`

   If the command returns `true`, on-access scanning will be started automatically with **`savd`** on system boot.

   Otherwise, type:

   `/opt/sophos-av/bin/savconfig set EnableOnStart true`

3.3 Start on-access scanning

To start on-access scanning, do one of the following:

- Type:
  `/opt/sophos-av/bin/savdctl enable`

- Use the appropriate tool to start the installed service sav-protect. For example, type:
  `/etc/init.d/sav-protect start`

or

```
service sav-protect start
```

3.4 Stop on-access scanning

Important: If you stop on-access scanning, Sophos Anti-Virus does not scan files that you access for viruses. This puts your computer, and others to which it is connected, at risk.

- To stop on-access scanning, type:
  `/opt/sophos-av/bin/savdctl disable`

4 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: Configuring scheduled scans (page 31).

4.1 Running on-demand scans

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

4.1.1 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.

4.1.2 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.

4.1.3 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.

4.1.4 Scan a boot sector

To scan a boot sector, log in as superuser. This grants you sufficient permission to access the disk devices.

You can scan the boot sector of a logical or physical drive.

- To scan the boot sector of specific logical drives, type:
  savscan -bs=*drive, drive, ...*

  where *drive* is the name of a drive, for example `/dev/fd0` or `/dev/hda1`.

- To scan the boot sector of all logical drives that Sophos Anti-Virus recognises, type:
  `savscan -bs`
- To scan the master boot record of all fixed physical drives on the computer, type:
  `savscan -mbr`

4.2 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`

4.2.1 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.

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.2.5 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**

4.2.6 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**.

4.2.7 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**

4.2.8 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

4.2.9 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**.

5 What happens if viruses are detected

Regardless of whether viruses are detected by on-access scanning or an on-demand scan, by default Sophos Anti-Virus:

- Logs the event in syslog and the Sophos Anti-Virus log (see View the Sophos Anti-Virus log (page 19)).
- Sends an alert to Enterprise Console if it is being managed by Enterprise Console.
- Sends an email alert to root@localhost.

By default, Sophos Anti-Virus also displays alerts according to whether the viruses were detected by on-access scanning or an on-demand scan, as explained below.

On-access scanning

If on-access scanning detects a virus, Sophos Anti-Virus denies access to the file and by default displays a desktop pop-up alert like the one shown below.

If the desktop pop-up alert cannot be displayed, a command-line alert is displayed instead.

For information about cleaning up viruses, see Cleaning up viruses (page 16).

On-demand scans

If an on-demand scan detects a virus, by default Sophos Anti-Virus 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 4.69.0 [Linux/Intel]
Virus data version 4.69
```

```
Includes detection for 2871136 viruses, Trojans and worms
Copyright (c) 1989-2012 Sophos Limited. All rights reserved.

System time 13:43:32, System date 22 September 2012

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 16).

6 Cleaning up viruses

6.1 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 (http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware.aspx).
2. Search for the analysis of the virus, by using the name that was reported by Sophos Anti-Virus.

6.2 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 17)) 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.

6.2.1 Specify quarantining

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

6.2.2 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.

6.3 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.

6.3.1 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 16) to find out how to view details on the Sophos website of the virus's side-effects.)

6.3.2 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 16) to find out how to view details on the Sophos website of the virus's side-effects.)

6.3.3 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.

6.3.4 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.

6.3.5 Disinfect an infected boot sector

- To disinfect an infected boot sector, use the disinfection option **-di** and the boot sector option **-bs**. For example, type:
  `savscan -bs=/dev/fd0 -di`

  where **`/dev/fd0`** is the name of the drive that contains the infected boot sector.

  Sophos Anti-Virus asks for confirmation before it disinfects.

6.4 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.

7 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, 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
  ```

8 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.

9 About kernel support

Note: This section is only applicable if you are using Talpa as your on-access scanning interception method. For more information, see Change the on-access scanning file interception method (page 45).

9.1 About 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 (Talpa) to support this. If you apply a Linux kernel update before you apply the matching Talpa update, Sophos Anti-Virus initiates a local compilation of Talpa. If this fails, Sophos Anti-Virus tries to use Fanotify as the interception method instead. If Fanotify is also unavailable, on-access scanning is stopped and an error is reported.

To avoid this problem, you must confirm that the matching Talpa update has been released before applying the Linux kernel update. A list of supported Linux distributions and updates is available in Sophos support knowledgebase article 14377 (http://www.sophos.com/en-us/support/knowledgebase/14377.aspx). When the required Talpa 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 Sophos Anti-Virus immediately, without waiting for the next automatic update, type:

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

You can then apply the Linux kernel update.

9.2 About support for customized kernels

If you customize your Linux kernels, this manual does not explain how to configure updating to support this. See Sophos support knowledgebase article 13503 (http://www.sophos.com/en-us/support/knowledgebase/13503.aspx).

10 Appendix: 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

10.1 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

Extended return code	Description
24	An item containing a virus is found and not disinfected
28	A virus is detected in memory
32	An integrity check failure occurs
36	An unsurvivable error occurs
40	The scan is interrupted

11 Appendix: Extra Files configuration

This section describes how to configure Sophos Anti-Virus with Extra Files configuration.

11.1 About Extra Files configuration

This section gives you an overview of Extra Files configuration.

11.1.1 What is Extra Files configuration?

Extra Files configuration is a method of configuring Sophos Anti-Virus for Linux. It is an alternative to configuration from Sophos Enterprise Console and it does not require a Windows computer.

You should use this method only if you cannot use Enterprise Console.

Note: You cannot use Enterprise Console configuration and Extra Files configuration together.

You can use this method to configure all features of Sophos Anti-Virus except on-demand scans, for which you should see Configuring on-demand scans (page 11)

11.1.2 How do you use Extra Files configuration?

You create a file that contains the Extra Files configuration settings. This file is offline, so that other computers cannot access it.

When you are ready to configure your computers, you copy the offline file to a live configuration file, which is in a location that endpoint computers can access. You configure each endpoint computer to fetch its configuration from the live file when that computer updates.

To reconfigure endpoint computers, you update the offline configuration file, and copy it to the live configuration file again.

Notes:

- To ensure that the configuration file is secure, you must create and use security certificates, as described in the following sections.
- You can lock part or all of the configuration so that individual end-users cannot modify it on their computer.

The following sections tell you how to create and use Extra Files configuration files.

11.2 Using Extra Files configuration

To use Extra Files, you:

- Create security certificates on the server.

- Create an Extra Files configuration.
- Install the root certificate on endpoint computers.
- Enable endpoint computers to use the Extra Files configuration.

11.2.1 Create security certificates on the server

You create the security certificates as follows.

Note: If you use OpenSSL to generate certificates, you must be running OpenSSL 0.9.8 or later.

1. Fetch the script that you will use to create the certificates. The script is available from Sophos support knowledgebase article 119602.
2. Run the script to create a set of certificates. For example, type:

   ```
   ./create_certificates.sh /root/certificates
   ```

   You can specify a different directory in which to place the certificates. However, you must ensure that the certificates are in a secure location.
3. When prompted, enter and confirm a root key password.
4. When prompted, enter and confirm a signing key password.
5. Check that the certificates are in the directory. Type:

   ```
   ls /root/certificates/
   ```

   You should see these files:

   ```
   extrafiles-root-ca.crt extrafiles-root-ca.key extrafiles-signing.cnf
   extrafiles-signing.crt extrafiles-signing.key
   ```

11.2.2 Create an Extra Files configuration

1. On the computer where you want to store the Extra Files configuration, use the command **savconfig** to create the offline configuration file and set the values of parameters in that file.

   Use the following syntax:

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

   where:

   - -f *offline-config-file-path* specifies the path of the offline configuration file, including the filename. **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 28)).
   - *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 `OfflineConfig.cfg` in the directory `/rootconfig/` and to disable email alerts, type:

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

   For information about using **savconfig**, see savconfig configuration command (page 29).

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 /root/config/OfflineConfig.cfg -c query

3. When you have finished setting parameters in the offline configuration file, create either a web share or a shared directory for storing the live configuration file.
4. Create the live configuration file by using the command **addextra**. Use the following syntax:

   /opt/sophos-av/update/addextra *offline-config-file-path live-config-file-path* **--signing-key=***signing-key-file-path* **--signing-certificate=***signing-certificate-file-path*

   For example:

   /opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /var/www/extrafiles/ --signing-key= /root/certificates/extrafiles-signing.key --signing-certificate=/root/certificates/extrafiles-signing.crt

11.2.3 Install the root certificate on endpoint computers

You must install the root certificate on each endpoint computer.

1. At the computer where you created the certificates (or the computer to which you copied them), create a new directory for the root certificate. Type:

   ```
   mkdir rootcert
   cd rootcert/
   ```

2. Copy the root certificate to the new directory. Type:

   ```
   cp /root/certificates/extrafiles-root-ca.crt .
   ```

3. Copy the new directory to a shared directory.
4. Go to each endpoint computer and mount the shared directory.
5. Install the certificate. Use the following syntax:

   `/opt/sophos-av/update/addextra_certs --install=` *`shared-rootcert-directory`*

   For example:

   ```
   /opt/sophos-av/update/addextra_certs --install= /mnt/rootcert/
   ```

11.2.4 Enable endpoint computers to use the Extra Files configuration

You enable the endpoint computers to download and use the configuration as follows.

1. If your live configuration file is in a shared directory, mount that directory on each client computer.
2. On each endpoint computer, specify the path of the live configuration file.
   For example:

   ```
   /opt/sophos-av/bin/savconfig set ExtraFilesSourcePath
   http://www.example.com/extrafiles
   ```

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

3. To run an update now, type:

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

11.3 Updating Extra Files configuration

1. On the computer where the Extra Files configuration is stored, use the command **`savconfig`** to update the offline configuration file and set the values of parameters in that file.

   You can use the same syntax as you did when creating the offline configuration file.

   For example, to update a file called `OfflineConfig.cfg` in the directory `/opt/sophos-av` and to enable email alerts, type:

   ```
   /opt/sophos-av/bin/savconfig -f /opt/sophos-av/OfflineConfig.cfg -c
   set EmailNotifier Enabled
   ```

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 /opt/sophos-av/OfflineConfig.cfg -c query

3. When you have finished setting parameters in the offline configuration file, update the live configuration file by using the command **addextra**. Use the following syntax:

   /opt/sophos-av/update/addextra *offline-config-file-path live-config-file-path* **--signing-key=***signing-key-file-path* **--signing-certificate=***signing-certificate-file-path*

   For example:

   /opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /var/www/extrafiles/ --signing-key= /root/certificates/extrafiles-signing.key --signing-certificate=/root/certificates/extrafiles-signing.crt

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

4. To run an update now, type:
   /opt/sophos-av/bin/savupdate

11.4 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 using Extra Files configuration.
- 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 Extra Files configuration file, the Corporate layer in the local file is replaced by that of the Extra Files configuration file.

11.5 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
```

11.5.1 *option*

You can specify one or more options. The options are mainly associated with the *layers* in the local configuration files in each installation. 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
```

11.5.2 *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”.

11.5.3 *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.

11.5.4 *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.

12 Appendix: 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 (http://www.sophos.com/en-us/support/knowledgebase/12176.aspx), 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.

12.1 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`

12.2 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.

12.3 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
  ```

12.4 Export names of all scheduled scans to a file

- To export the names of all scheduled scans (including those that have been created using Enterprise 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.

12.5 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
  ```

12.6 Export names of all scheduled scans to standard output

- To export the names of all scheduled scans (including those that have been created using Enterprise 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.

12.7 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 32).

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
   ```

12.8 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.

12.9 View log of a scheduled scan

- To view the log of a scheduled scan, use the command **`savlog`** and the option **namedscan**. Specify the name of the scan.

  For example, to view the log of the scan Daily, type:

```
/opt/sophos-av/bin/savlog --namedscan=Daily
```

12.10 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
  ```

12.11 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

13 Appendix: Configuring 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 Enterprise Console configuration or Extra Files configuration.

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

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

Desktop pop-up and command-line alerts are sent in the language of the computer that raises the alert. Email alerts can be sent in English or Japanese.

13.1 Configuring desktop pop-up alerts

13.1.1 Turn off desktop pop-up alerts

By default, desktop pop-up alerts are turned on.

- To turn off desktop pop-up alerts, type:
  `/opt/sophos-av/bin/savconfig set UIpopupNotification disabled`
- To turn off both desktop pop-up and command-line alerts, type:
  `/opt/sophos-av/bin/savconfig set UINotifier disabled`

13.1.2 Specify custom message

You can specify a custom message that will be added to all command-line alerts and desk-top pop-up alerts.

Remember: The main alert message can be displayed in different languages (depending on the system settings), but the custom text will stay in the language you used when you specified it.

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

13.2 Configuring command-line alerts

13.2.1 Turn off command-line alerts

By default, command-line alerts are turned on.

- To turn off command-line alerts, type:
  `/opt/sophos-av/bin/savconfig set UIttyNotification disabled`
- To turn off both desktop pop-up and command-line alerts, type:
  `/opt/sophos-av/bin/savconfig set UINotifier disabled`

13.2.2 Specify custom message

You can specify a custom message that will be added to all command-line alerts and desk-top pop-up alerts.

Remember: The main alert message can be displayed in different languages (depending on the system settings), but the custom text will stay in the language you used when you specified it.

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

13.3 Configuring email alerts

13.3.1 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`

13.3.2 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`

13.3.3 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.

13.3.4 Specify the email recipients

By default, email alerts are sent 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

  Important: You cannot remove **root@localhost** with this command. To do this, you must overwrite the list completely with the following command:
  /opt/sophos-av/bin/savconfig set Email <email addresses>

13.3.5 Specify the email Sender address

By default, email alerts are sent from root@localhost.

- To specify an email Sender address, use the parameter **EmailSender**. For example, type:
  /opt/sophos-av/bin/savconfig set EmailSender admin@localhost

13.3.6 Specify the email ReplyTo address

- To specify an email ReplyTo address, use the parameter **EmailReplyTo** . For example, type:
  /opt/sophos-av/bin/savconfig set EmailReplyTo admin@localhost

13.3.7 Specify what happens if viruses are detected on-access

By default, Sophos Anti-Virus sends an email alert if on-access scanning detects viruses. 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 turn off the sending of email alerts if viruses are detected on-access, type:

```
/opt/sophos-av/bin/savconfig set SendThreatEmail disabled
```

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

13.3.8 Specify what happens if there is an on-access scanning error

By default, Sophos Anti-Virus sends an email alert if there is an on-access scanning error. 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 turn off the sending of email alerts if there is an on-access scanning error, type:

  `/opt/sophos-av/bin/savconfig set SendErrorEmail disabled`

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

13.3.9 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`

13.3.10 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'`

14 Appendix: 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 Enterprise Console configuration or Extra Files 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`

15 Appendix: 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.

15.1 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.

15.2 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
```

15.3 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 **Auto-updating configuration**.

   `savsetup` asks you to select what you want to do.

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

15.4 Configure an update server

You can use any standalone Sophos Anti-Virus installation as an update server for other network computers.

Note:

The update server must be a 64-bit computer if it is used to keep any 64-bit clients up to date. If the update server is a 32-bit computer, it does not download 64-bit updates, and cannot update the clients.

1. At the update server, type:
   `/opt/sophos-av/bin/savsetup`

   `savsetup` asks you to select what you want to do.

2. Select an option and follow the prompts to configure the update server.

   When configuring updates, if you are updating from Sophos, enter the username and password that are included with your license. If you are updating from an update server, you can specify either an HTTP address or a UNC path, depending on how you have set up the update server.

3. To host updates for other Sophos Anti-Virus clients:

   a) Copy the local cache directory (/opt/sophos-av/update/cache/) to a different location on the filesystem.

      This can be automated using a script.

   b) Publish the location to other networked computers via HTTP, SMB, NFS or other method.

      This location will be the central installation directory (CID) from where the clients will download updates.

15.5 Configure multiple update clients to update

This section explains how to change the update parameters in the Extra Files configuration. The configuration is then downloaded by the update clients the next time that they update.

This section assumes that you have already created the Extra Files configuration. If it is not created, see Appendix: Extra Files configuration (page 24).

Note: This section describes how to configure multiple update clients to update from the *primary* update source. You can use the same procedure to configure your *secondary* update source by replacing *Primary* with *Secondary*. For example, instead of **PrimaryUpdateSourcePath** use **SecondaryUpdateSourcePath**.

To configure multiple update clients to update:

1. At the computer where the Extra Files configuration is stored, set the update source address either to **sophos:** or the location of the central installation directory (CID) using the parameter **PrimaryUpdateSourcePath**.

   To update from the CID, 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 *offline-config-file-path* **-c set PrimaryUpdateSourcePath 'http://www.mywebcid.com/cid'**

   To update from **sophos:**, type:

   /opt/sophos-av/bin/savconfig -f *offline-config-file-path* **-c set PrimaryUpdateSourcePath 'sophos:'**

2. If the 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 *offline-config-file-path* **-c set PrimaryUpdateUsername 'fred'**

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

3. If you access the 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 *offline-config-file-path* **-c set PrimaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'**

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

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

4. When you have finished setting parameters in the offline configuration file, update the live configuration file by using the command **addextra**. Use the following syntax:

   /opt/sophos-av/update/addextra *offline-config-file-path live-config-file-path* **--signing-key=***signing-key-file-path* **--signing-certificate=***signing-certificate-file-path*

   For example:

   /opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /var/www/extrafiles/ --signing-key= /root/certificates/extrafiles-signing.key --signing-certificate=/root/certificates/extrafiles-signing.crt

The updated configuration is now available for the update clients to download the next time that they update.

15.6 Configure a single update client to update

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 an option and follow the prompts to configure the update client.

   When configuring updates, if you are updating from Sophos, enter the username and password that are included with your license. If you are updating from an update server, you can specify either an HTTP address or a UNC path, depending on how you have set up the update server.

16 Appendix: Configuring Sophos Live Protection

Note: If you are configuring a single computer that is on a network, the configuration might be overwritten if the computer downloads a new Enterprise Console configuration or Extra Files configuration.

Sophos Live Protection decides whether a suspicious file is a threat and, if it is a threat, takes immediate action as specified in the Sophos Anti-Virus cleanup configuration.

Live Protection improves detection of new malware without the risk of unwanted detections. This is achieved by doing an instant lookup against the very latest known malware. When new malware is identified, Sophos can send out updates within seconds.

If the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on the computer, certain file data (such as its checksum and other attributes) is sent to Sophos to assist with further analysis.

The in-the-cloud checking performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated.

16.1 Check Sophos Live Protection setting

Sophos Live Protection is turned on by default if you have installed Sophos Anti-Virus for the first time. If you have upgraded from a previous version of Sophos Anti-Virus, it is turned off.

- To check the Live Protection setting, type:
  `/opt/sophos-av/bin/savconfig query LiveProtection`

16.2 Turn Sophos Live Protection on or off

- To turn on Live Protection, type:

  `/opt/sophos-av/bin/savconfig set LiveProtection true`

- To turn off Live Protection, type:

  `/opt/sophos-av/bin/savconfig set LiveProtection false`

17 Appendix: Configuring on-access scanning

Note: If you are configuring a single computer that is on a network, the configuration might be overwritten if the computer downloads a new Enterprise Console configuration or Extra Files configuration.

17.1 Change the on-access scanning file interception method

If you upgrade to a version of Linux kernel that does not support Talpa, you can use Fanotify as your on-access scanning file interception method.

Important: Use of Fanotify by Sophos Anti-Virus is beta functionality that is not fully supported.

- To use Fanotify as your on-access scanning file interception method, type:
  `/opt/sophos-av/bin/savconfig set DisableFanotify false`

17.2 Excluding files and directories from scanning

You can exclude files and directories from scanning in two ways:

- Using file or directory name
- Using wildcards

If you want to exclude files and directories whose names are encoded using non-UTF-8, see Specifying character encoding of directory names and filenames (page 46).

17.2.1 Use file or directory name

Note: If you are configuring a single computer that is on a network, the configuration might be overwritten if the computer downloads a new Enterprise Console configuration or Extra Files configuration.

- To exclude a particular file or directory, use the **ExcludeFilePaths** parameter with the **add** operation. Specify a directory by using a trailing slash. For example, to add the file `/tmp/report` to the list of files and directories to exclude, type:
  `/opt/sophos-av/bin/savconfig add ExcludeFilePaths /tmp/report`

  To add the directory `/tmp/report/` to the list of files and directories to exclude, type:

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

- To remove an exclusion from the list, use the **ExcludeFilePaths** parameter with the **remove** operation. For example, type:

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

17.2.2 Use wildcards

Note: If you are configuring a single computer that is on a network, the configuration might be overwritten if the computer downloads a new Enterprise Console configuration or Extra Files configuration.

- To exclude files and directories by using wildcards, use the **ExcludeFileOnGlob** parameter with the **add** operation. 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 add ExcludeFileOnGlob '/tmp/*.txt'`

  Note: If you use ExcludeFileOnGlob to exclude **a directory**, you must add the * wildcard to the end of the path. For example:

  `/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob '/tmp/report/*'`

- If you do not enclose the expression in quotation marks, Linux expands the expression and passes the list of files to Sophos Anti-Virus. This is useful for excluding only files that exist already, and enabling files that are created later to be scanned. For example, to add just text files that exist already in the `/tmp` directory to the list of files and directories to exclude, type:
  `/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob /tmp/*.txt`

- To remove an exclusion from the list, use the **ExcludeFileOnGlob** parameter with the **remove** operation. For example, type:
  `/opt/sophos-av/bin/savconfig remove ExcludeFileOnGlob '/tmp/notes.txt'`

17.2.3 Specifying character encoding of directory names and filenames

Linux enables you to name directories and files using any character encoding that you choose (for example, UTF-8, EUC_jp). However, Sophos Anti-Virus stores exclusions only in UTF-8. Therefore, if you want to exclude directories and files from scanning whose names are encoded using non-UTF-8, you specify the exclusions in UTF-8, and specify the encodings using the **ExclusionEncodings** parameter. Then, the names of any directories or files that you exclude are evaluated in each of the encodings that you specified, and all matching directories and files are excluded. This applies to exclusions that have been specified using the **ExcludeFilePaths** and **ExcludeFileOnGlob** parameters. By default, UTF-8, EUC_jp, and ISO-8859-1 (Latin-1) are specified.

For example, if you want to exclude directories and files whose names are encoded in EUC_cn, you specify the names of the directories and files using the **ExcludeFilePaths** and/or the **ExcludeFileOnGlob** parameter. Then, you add EUC_cn to the list of encodings:

`/opt/sophos-av/bin/savconfig add ExclusionEncodings EUC_cn`

Then, Sophos Anti-Virus evaluates in UTF-8, EUC_jp, ISO-8859-1 (Latin-1), and EUC_cn all the directory names and filenames that you specified. It then excludes all directories and files whose names match.

17.3 Exclude a filesystem type from scanning

By default, no filesystem types are excluded.

- To exclude a filesystem type, use the **ExcludeFilesystems** parameter with the **add** operation. 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 add ExcludeFilesystems nfs`

- To remove an exclusion from the list, use the **ExcludeFilesystems** parameter with the **remove** operation. For example, type:
  `/opt/sophos-av/bin/savconfig remove ExcludeFilesystems nfs`

17.4 Scan inside archives

By default, on-access scanning inside archives is turned off. However, you might want to turn on the option if you are dealing with several such files at a time and the cost of not detecting a virus is high. For example, you might be emailing some archives to an important contact.

Note: We recommend that you do not turn on this option, for the following reasons:

- Scanning inside archives makes scanning significantly slower.
- Whether you turn on this option or not, when you open a file extracted from an archive, the extracted file is scanned.
- To turn *on* scanning inside archives, type:
  `/opt/sophos-av/bin/savconfig set ScanArchives enabled`

- To turn *off* scanning inside archives, type:
  `/opt/sophos-av/bin/savconfig set ScanArchives disabled`

17.5 Cleaning up infected files

You can configure on-access scanning to clean up (disinfect or delete) infected files. By default, cleanup is disabled.

Any actions that Sophos Anti-Virus takes against infected files are logged in the Sophos Anti-Virus log.

Note: You can turn on both disinfection and deletion, but we do not recommend it. If you do this, Sophos Anti-Virus first tries to disinfect the file. If disinfection fails, it deletes it.

Note: Sophos Anti-Virus can disinfect or delete files when scanning "on open" (i.e. when files are copied, moved or opened). It cannot do so when scanning "on close" (i.e. when files are saved or created). This is not an issue in normal use, as "on open" scanning cannot be centrally disabled on Linux computers, and will disinfect or delete files on the next access.

17.5.1 Disinfect infected files and boot sectors

- To turn *on* disinfection of infected files and boot sectors on-access, type:
  `/opt/sophos-av/bin/savconfig add AutomaticAction disinfect`

  Important: Sophos Anti-Virus does not ask 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 16) to find out how to view details on the Sophos website of the virus's side-effects.)

- To turn *off* disinfection of infected files and boot sectors on-access, type:
  `/opt/sophos-av/bin/savconfig remove AutomaticAction disinfect`

17.5.2 Delete infected files

Important: 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 turn *on* deletion of infected files on-access, type:
  `/opt/sophos-av/bin/savconfig add AutomaticAction delete`

  Important: Sophos Anti-Virus does not ask for confirmation before it deletes.

- To turn *off* deletion of infected files on-access, type:
  `/opt/sophos-av/bin/savconfig remove AutomaticAction delete`

18 Appendix: Configuring the phone-home feature

Sophos Anti-Virus can contact Sophos and send us some product and platform details. This "phone-home" feature helps us to improve the product and user experience.

When you install Sophos Anti-Virus, the phone-home feature is turned on by default. We would like you to leave it on. It doesn't affect your security or your computer performance:

- Your data is sent in encrypted form to a secure location and we keep it for no more than three months.
- The product sends only about 2 KB of data once a week. It phones home at random intervals, to avoid multiple computers phoning home at the same time.

You can turn off the feature at any time after installation.

To turn off the phone-home feature, type:

```
/opt/sophos-av/bin/savconfig set DisableFeedback true
```

To turn on the phone-home feature again, type:

```
/opt/sophos-av/bin/savconfig set DisableFeedback false
```

19 Appendix: Configuring restarts for RMS

If RMS (Remote Management System), which handles communications with the server, crashes or does not start properly, an adapter restarts the RMS components, mrouter and magent.

If you want to restart RMS periodically, add

`RestartIntervalHours=<Hours>`

to $INST/etc/sophosmgmtd.conf.

20 Troubleshooting

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

For information about Sophos Anti-Virus return codes for on-demand scans, see Appendix: On-demand scan return codes (page 22).

20.1 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.

20.2 Exclusion configuration has not been applied

Symptom

Occasionally, when you configure Sophos Anti-Virus to include files for on-access scanning that were previously excluded, the files remain excluded.

Cause

This might be because the cache of files that have previously been scanned still includes the files that were previously excluded.

Resolve the problem

Depending on the on-access scanning interception method you are using, do one of the following:

- If you are using Talpa, try flushing the cache. To do this, type:

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

- If you are using Fanotify, try restarting the installed service sav-protect. To do this, type:

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

20.3 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.

20.4 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.

20.5 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 11).

20.6 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**.

20.7 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.

20.8 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 17).
3. If virus fragments are still reported, contact Sophos technical support for advice.

20.9 Unable to access disk

Symptom

You are unable to access files on a removable disk.

Cause

By default, Sophos Anti-Virus prevents access to removable disks whose boot sectors are infected.

Resolve the problem

To allow access (for example to copy files from a floppy disk infected with a boot sector virus):

1. Type:

   ```
   /opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat enabled
   ```

2. When you have finished accessing the disk, type:

```
/opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat disabled
```

3. Remove the disk from the computer so that it cannot try to re-infect the computer on restart.

21 Glossary

boot sector virus	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 partition boot sector.
central installation directory (CID)	A directory into which Sophos software and updates are placed. Networked computers update themselves from this directory.
disinfection	Disinfection removes a virus from a file or boot sector.
Extra Files	A location used to store Sophos Anti-Virus configuration for a network. When computers update, they download the configuration from this location.
on-access scan	Your main method of protection against viruses. Whenever you access (copy, save, move, or open) a file, Sophos Anti-Virus scans the file and grants access to it only if it does not pose a threat to your computer.
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.
Sophos Live Protection	A feature that uses in-the-cloud technology to instantly decide whether a suspicious file is a threat and take action specified in the Sophos Anti-Virus cleanup configuration.
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.

22 Technical support

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

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

23 Legal notices

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, 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. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

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

Douglas C. 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.

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.

OpenSSL Cryptography and SSL/TLS 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 © 1998–2011 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 license 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 license [including the GNU Public License.]

Protocol Buffers (libprotobuf)

Copyright 2008, Google Inc.

All rights reserved.

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

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 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.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS 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 COPYRIGHT OWNER 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.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

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

www.sourceforge.net/projects/tinyxml

Original code by Lee Thomason (www.grinninglizard.com)

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 data compression library

Copyright © 1995–2013 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 jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

Index

Q

R

S

U

V