SOPHOS
Security made simple.

Sophos Anti-Virus for Unix

configuration guide

Product Version: 9

Contents

About this guide.. 1
About Sophos Anti-Virus for UNIX..2
What Sophos Anti-Virus does..2
How Sophos Anti-Virus protects your computer..2
How you use Sophos Anti-Virus..2
How you configure Sophos Anti-Virus.. 2
On-demand scanning..4
Running on-demand scans.. 4
Configuring on-demand scans.. 4
What happens if viruses are detected..8
Cleaning up viruses.. 9
Get cleanup information.. 9
Quarantining infected files..9
Cleaning up infected files.. 10
Recovering from virus side-effects..11
View the Sophos Anti-Virus log..12
Update Sophos Anti-Virus immediately..13
Appendix: On-demand scan return codes.. 14
Extended return codes..14
Appendix: Extra Files configuration..15
About Extra Files configuration..15
Using Extra Files configuration.. 15
Updating Extra Files configuration..18
About configuration layers..18
savconfig configuration command..19
Appendix: Configuring scheduled scans.. 21
Add a scheduled scan from a file..21
Add a scheduled scan from standard input..21
Export a scheduled scan to a file..22
Export names of all scheduled scans to a file.. 22
Export a scheduled scan to standard output..22
Export names of all scheduled scans to standard output..22
Update a scheduled scan from a file.. 23
Update a scheduled scan from standard input.. 23
View the Sophos Anti-Virus log.. 24
Remove a scheduled scan..24
Remove all scheduled scans.. 24
Appendix: Configuring email alerts.. 25
Turn off email alerts..25
Specify the SMTP server hostname or IP address.. 25
Specify the language..25
Specify the email recipients..25
Specify the email Sender address.. 26
Specify the email ReplyTo address.. 26
Turn on-demand email alerts off..26
Specify what happens if an event is logged..26
Appendix: Configure logging.. 27
Appendix: Syslog messages.. 28
Appendix: Configuring updating.. 40
Basic concepts..40
savsetup configuration command..40
Check the auto-updating configuration for a computer..41

Configure multiple update clients to update from Sophos directly when the update server is unavailable......41
Configure a single update client to update from the update server......42
Appendix: Configuring the phone-home feature......43
Troubleshooting......44
Unable to run a command......44
Computer reports “No manual entry for ...”......44
Runs out of disk space......45
On-demand scanning runs slowly......45
Archiver backs up all files that have been scanned on demand......46
Virus not cleaned up......47
Virus fragment reported......47
Glossary......49
Technical support......50
Legal notices......51

Index......57

1 About this guide

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

To *install* Sophos Anti-Virus, see the *Sophos Anti-Virus for UNIX startup guide*.

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

2 About Sophos Anti-Virus for UNIX

2.1 What Sophos Anti-Virus does

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

2.2 How Sophos Anti-Virus protects your computer

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

2.3 How you use Sophos Anti-Virus

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

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

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

2.4 How you configure Sophos Anti-Virus

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

- Configure **scheduled scans, alerting, logging, and updating** centrally by editing a configuration file from which the computers update. See Appendix: Extra Files configuration (page 15).
- Configure **on-demand scans** from the Sophos Anti-Virus command-line interface on each computer locally.

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

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

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

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

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

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

3 On-demand scanning

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

To schedule an on-demand scan, use the command `crontab`. For details, see Sophos support knowledgebase article 12176.

3.1 Running on-demand scans

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

3.1.1 Run an on-demand scan of the computer

We recommend that you scan the whole computer for viruses right after you install Sophos Anti-Virus. To do this, you run an on-demand scan.

Note

This is especially important if the computer is a server and you want to minimize the risk of spreading viruses to other computers.

- To run an on-demand scan of the computer, type:

  ```
  savscan /
  ```

3.1.2 Scan a particular directory or file

- To scan a particular directory or file, specify the path of the item. For example, type:

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

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

3.1.3 Scan a filesystem

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

  ```
  savscan /home
  ```

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

3.2 Configuring on-demand scans

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

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

```
man savscan
```

3.2.1 Scan all file types

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

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

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

3.2.2 Scan a particular directory or file

- To scan a particular directory or file, specify the path of the item. For example, type:
  `savscan /usr/mydirectory/myfile`
  You can type more than one directory or file in the same command.

3.2.3 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`.

> **Note**
> The threat detection engine only scans archived files that are up to 8GB (when decompressed). This is because it supports the POSIX ustar archive format, which does not accommodate larger files.

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

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

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

3.2.4 Scan inside a particular archive type

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

Note

The threat detection engine only scans archived files that are up to 8GB (when decompressed). This is because it supports the POSIX ustar archive format, which does not accommodate larger files.

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

  ```
  savscan path -tar -zip
  ```

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

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

3.2.5 Scan remote computers

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

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

  ```
  savscan path --no-stay-on-machine
  ```

3.2.6 Turn off scanning of symbolically linked items

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

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

  ```
  savscan path --no-follow-symlinks
  ```

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

3.2.7 Scan the starting filesystem only

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

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

  ```
  savscan path --stay-on-filesystem
  ```

3.2.8 Excluding items from scanning

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

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

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

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

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

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

3.2.9 Scan file types that UNIX defines as executables

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

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

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

4 What happens if viruses are detected

If viruses are detected, by default Sophos Anti-Virus:

- Logs the event in syslog and the Sophos Anti-Virus log (see View the Sophos Anti-Virus log (page 12)).
- 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.

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 9).

5 Cleaning up viruses

5.1 Get cleanup information

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

To get cleanup information:

1. Go to the security analyses page (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.

5.2 Quarantining infected files

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

Note
If you specify disinfection (see Cleaning up infected files (page 10)) as well as quarantining, Sophos Anti-Virus attempts to disinfect infected items and quarantines them only if disinfection fails.

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

5.2.1 Specify quarantining

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

5.2.2 Specifying the ownership and permissions that are applied

By default, Sophos Anti-Virus changes:

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

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

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

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

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

For example:

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

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

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

5.3 Cleaning up infected files

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

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

5.3.1 Disinfect a specific infected file

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

  Sophos Anti-Virus asks for confirmation before it disinfects.

> **Note**
> Disinfecting an infected document does not repair any changes the virus has made to the document. (See Get cleanup information (page 9) to find out how to view details on the Sophos website of the virus's side-effects.)

5.3.2 Disinfect all infected files on the computer

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

  Sophos Anti-Virus asks for confirmation before it disinfects.

> **Note**
> Disinfecting an infected document does not repair any changes the virus has made to the document. (See Get cleanup information (page 9) to find out how to view details on the Sophos website of the virus's side-effects.)

5.3.3 Delete a specific infected file

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

  Sophos Anti-Virus asks for confirmation before it deletes.

5.3.4 Delete all infected files on the computer

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

  Sophos Anti-Virus asks for confirmation before it deletes.

5.4 Recovering from virus side-effects

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

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

Sound backups are crucial. If you did not have them before you were infected, start keeping them in case of future infections.

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

6 View the Sophos Anti-Virus log

Sophos Anti-Virus logs details of scanning activity in the Sophos Anti-Virus log and syslog. In addition, virus and error events are logged in the Sophos Anti-Virus log.

For further information on the information logged in syslog see Appendix: Syslog messages (page 28).

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

  For example, to display all messages logged to the Sophos Anti-Virus log in the last 24 hours, and to display the date and time in UTC/ISO 8601 format, type:

  ```
  /opt/sophos-av/bin/savlog --today --utc
  ```
- To see a complete list of the options that can be used with `savlog`, type:
  ```
  man savlog
  ```

7 Update Sophos Anti-Virus immediately

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

- To update Sophos Anti-Virus immediately, at the computer that you want to update, type:

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

Note

You can also update computers immediately from Sophos Enterprise Console.

8 Appendix: On-demand scan return codes

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

```
echo $?
```

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

8.1 Extended return codes

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

```
echo $?
```

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

9 Appendix: Extra Files configuration

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

9.1 About Extra Files configuration

This section gives you an overview of Extra Files configuration.

9.1.1 What is Extra Files configuration?

Extra Files configuration is a method of configuring Sophos Anti-Virus. 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 4)

9.1.2 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.

9.2 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.

9.2.1 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
   ```

9.2.2 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 18)).
   - *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 19).

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
   ```

9.2.3 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/
   ```

9.2.4 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
   ```

9.3 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
   ```

9.4 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.

9.5 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
```

9.5.1 *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
```

9.5.2 *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”.

9.5.3 *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.

9.5.4 *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.

10 Appendix: Configuring scheduled scans

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

> **Note**
> Scheduled scans that have been added using Enterprise Console have names that are prefixed with "SEC:" and cannot be updated or removed except by using Enterprise Console.

10.1 Add a scheduled scan from a file

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

   To create a scan definition from scratch, open a new text file.
2. Define what to scan, when to scan it, and any other options, using only the parameters listed in the template.

   To schedule the scan, you must include at least one day and one time.
3. Save the file in a location of your choosing, being careful not to overwrite the template.
4. Add the scheduled scan to Sophos Anti-Virus using the command `savconfig` with the operation add and the parameter NamedScans. Specify the name of the scan and the path of the scan definition file.

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

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

10.2 Add a scheduled scan from standard input

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

   For example, to add the scan Daily, type:

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

   When you press ENTER, Sophos Anti-Virus waits for you to type the definition of the scheduled scan.
2. Define what to scan, when to scan it, and any other options, using only the parameters listed in the template scan definition: `/opt/sophos-av/doc/namedscan.example.en`. After typing each parameter and its value, press ENTER.

   To schedule the scan, you must include at least one day and one time.
3. To complete the definition, press CTRL+D.

10.3 Export a scheduled scan to a file

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

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

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

10.4 Export names of all scheduled scans to a file

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

10.5 Export a scheduled scan to standard output

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

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

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

10.6 Export names of all scheduled scans to standard output

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

10.7 Update a scheduled scan from a file

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

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

   If the scan is not already defined in a file, you can export the scan to a file, as explained in Export a scheduled scan to a file (page 22).
2. Amend the definition as necessary, using only the parameters listed in the template scan definition: `/opt/sophos-av/doc/namedscan.example.en`. You must define the scan completely, instead of just specifying what you want to update.
3. Save the file.
4. Update the scheduled scan in Sophos Anti-Virus using the command `savconfig` with the operation update and the parameter NamedScans. Specify the name of the scan and the path of the scan definition file.

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

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

10.8 Update a scheduled scan from standard input

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

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

   For example, to update the scan Daily, type:

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

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

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

3. 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.

10.9 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.

For further information on the information logged in syslog see Appendix: Syslog messages (page 28).

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

  For example, to display all messages logged to the Sophos Anti-Virus log in the last 24 hours, and to display the date and time in UTC/ISO 8601 format, type:

  ```
  /opt/sophos-av/bin/savlog --today --utc
  ```
- To see a complete list of the options that can be used with `savlog`, type:
  ```
  man savlog
  ```

10.10 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
  ```

10.11 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
  ```

11 Appendix: Configuring email alerts

Note

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

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

11.1 Turn off email alerts

By default, email alerts are turned on.

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

11.2 Specify the SMTP server hostname or IP address

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

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

11.3 Specify the language

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

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

Note

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

11.4 Specify the email recipients

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

- To add an address to the list of recipients of email alerts, use the parameter Email with the operation add. For example, type:

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

Note

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

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

11.5 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
  ```

11.6 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
  ```

11.7 Turn on-demand email alerts off

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

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

11.8 Specify what happens if an event is logged

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

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

12 Appendix: 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.

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

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

13 Appendix: Syslog messages

Sophos Anti-Virus logs three types of messages in syslog. These are:

- `ACTION-REQUIRED`: These messages show when you need to take remedial action.
- `ERROR`: These messages detail errors encountered during scanning.
- `INFO`: These messages provide information on the scanning process.

Messages are listed in order of severity.

Action required messages

You need to take remedial action for the following messages.

Syslog Message	Description	Message ID	Notes
"The threat data is out of date and should be updated."	The threat data is out of date and should be updated.	`VIRUS-DATA-OLD`	This means that your updating source is not getting updates from Sophos. You should investigate to ensure that timely updates from Sophos are being delivered.
"Sophos Anti-Virus is not configured to update."	Sophos Anti-Virus is not configured to update.	`NO-UPDATE-CONFIGURATION`	Sophos Anti-Virus is only providing useful protection if it is getting updates from Sophos, this machine is not configured to update.
"Not updating from Sophos as updates directly from Sophos are not supported."	Not updating from Sophos as updates directly from Sophos are not supported.	`NO-UPDATE-FROM-SOPHOS`	This is a legacy message and should never appear.
"Threat detected in %s: %s during on-demand scan. (The file is still infected.)"	Sophos Anti-Virus detected a threat during an on-demand scan. The file is still infected.	`NOTIFY-ONDEMAND-THREAT-INFECTED`	You need to log in and remove the file, or use savscan to attempt disinfection.

Syslog Message	Description	Message ID	Notes
"Threat detected in %s: %s during on-demand scan. (The file has been quarantined.)"	Sophos Anti-Virus detected a threat during an on-demand scan. The file is still infected. The file is not executable and not accessible to normal users if the scan was run as root.	`NOTIFY-ONDEMAND-THREAT-QUARANTINED`	You need to log in and remove the file, or use savscan to attempt disinfection.

Error messages

These messages detail errors that occurred during the scanning process. They also tell you what remedial action you need to take, if any.

Syslog Message	Description	Message ID
"Too many incidents occurred (%s incident notifications were discarded)."	Too many incidents occurred (%s incident notifications were discarded). This indicates that savd was overloaded with notifications, and some have been discarded.	`MESSAGES_DROPPED %s`
"Respawn limit exceeded[no further scan processors will be started."	Respawn limit exceeded no further scan processors will be started. savd has stopped spawning savscand due to failures to start savscand. Restart savd once the problem has been rectified.	`RESPAWN-LIMIT`
"Throttling scan processor respawn."	Savd is controlling how fast savscand processes are started, as they are exiting too fast.	`RESPAWN-THROTTLE`
"Previous instance of Sophos Anti-Virus daemon did not exit cleanly."	Sophos Anti-Virus did not shut down properly last time. No further action needed.	`SAVD-CLEANUP`
"Force-terminated a scan processor."	Sophos Anti-Virus scanner terminated. Savd forceably stopped a savscand. No further action needed unless this happens frequently.	`SCANNER-DIED-KILLED`

Syslog Message	Description	Message ID
"Force-terminated a scan processor."	Sophos Anti-Virus scanner terminated. Savd forceably stopped a savscand. No further action needed unless this happens frequently.	`SCANNER-DIED-KILLED-PID`
"A scan processor unexpectedly terminated with signal: %s."	Sophos Anti-Virus scanner terminated. A savscand terminated due to receiving a signal. No further action needed unless this happens frequently.	`SCANNER-DIED-SIGNAL`
"A scan processor died during startup with signal: %s."	Sophos Anti-Virus scanner did not start. A savscand terminated due to receiving a signal during startup. No further action needed unless this happens frequently.	`SCANNER-DIED-STARTUP-SIGNAL`
"A scan processor died during startup with status code: %s."	Sophos Anti-Virus scanner did not start. A savscand exited during startup. No further action needed unless this happens frequently.	`SCANNER-DIED-STARTUP-STATUS`
"A scan processor unexpectedly terminated with status code: %s."	Sophos Anti-Virus scanner terminated unexpectedly. A savscand unexpectedly exited. No further action required unless this happens frequently.	`SCANNER-DIED-STATUS`
"Terminated a scan processor."	Sophos Anti-Virus scanner terminated. Savd terminated a savscand. No further action needed unless this happens frequently.	`SCANNER-DIED-TERMED`
"Terminated a scan processor."	Sophos Anti-Virus scanner terminated. Savd terminated a savscand. No further action needed unless this happens frequently.	`SCANNER-DIED-TERMED-PID`

Syslog Message	Description	Message ID
"Scan processor failed to send heartbeat messages and will be stopped."	Sophos Anti-Virus didn't send heartbeat messages and stopped. A savscand failed to send heartbeat messages in time. Savd terminated it. No further action needed unless this happens frequently.	`TIMEOUT-SCANNER-HEARTBEAT`
"A scan processor timed out during startup."	Sophos Anti-Virus timed out and didn't start. A savscand failed to start in time. Savd terminated it. No further action needed unless this happens frequently.	`TIMEOUT-SCANNER-STARTUP`
"Threat detected in %s: %s during on-demand scan. (The file has been deleted.)"	Sophos Anti-Virus detected a threat during an on-demand scan. The file has been deleted.	`NOTIFY-ONDEMAND-THREAT-DELETED`
"Threat detected in %s: %s during on-demand scan. (The file has been disinfected.)"	Sophos Anti-Virus detected a threat during an on-demand scan. The file has been disinfected.	`NOTIFY-ONDEMAND-THREAT-DISINFECTED`
"On-demand scan aborted by user."	Sophos Anti-Virus scan stopped by user.	`SAVSCAN-ABORTED`
"Scheduled scan \"%s\" failed with error %s (%s)."	Sophos Anti-Virus scheduled scan failed with an error. The scan will be attempted again at the next scheduled interval.	`SCHEDULED-SCAN-FAILED`
"Scheduled scan \"%s\" failed: unable to parse mounts."	Sophos Anti-Virus scheduled scan failed as it was unable to parse the mount table. If this repeats please report the problem to Sophos Support. Please check 'mount' output.	`SCHEDULED-SCAN-FAILED-MOUNT-PARSING`
"Scheduled scan \"%s\" failed: unable to load threat data (%s)."	Sophos Anti-Virus scheduled scan failed while loading threat data. No action required unless scan repeatedly fails.	`SCHEDULED-SCAN-FAILED-VDL-LOAD-ERROR`

Syslog Message	Description	Message ID
"Unable to load threat data (%s)."	Sophos Anti-Virus failed while loading threat data. No action required unless this message is repeated.	`SAVI_VDL_LOAD_ERROR`
"Failed to replicate from all update sources."	Sophos Anti-Virus failed to update. No action required unless this message is repeated. If it fails repeatedly check the primary update settings are correct.	`ALL_UPDATE` `_SOURCES_FAILED`
"Failed to download '%s': invalid authentication."	Sophos Anti-Virus didn't update. No action required unless this message is repeated. If it fails repeatedly check the primary update settings are correct.	`BAD-BACKUP-AUTHENTICATION`
"Failed to download '%s': invalid proxy authentication."	Sophos Anti-Virus didn't update. No action required unless this message is repeated. If it fails repeatedly check the primary update settings are correct.	`BAD-BACKUP-PROXY-AUTHENTICATION`
"Failed to download '%s': no such file."	Sophos Anti-Virus can't update. No action required unless this message is repeated. If it fails repeatedly check the primary update settings are correct.	`BAD-BACKUP-URL`
"Failed to download '%s': invalid authentication. Please check `ExtraFilesUsername` and `ExtraFilesPassword`."	Sophos Anti-Virusfailed to download `ExtraFiles`. No action required unless this message is repeated. If it fails repeatedly check `ExtraFilesUsername` and `ExtraFilesPassword` are correct.	`BAD-EXTRAFILES-AUTHENTICATION`
"Failed to download '%s': invalid proxy authentication. Please check `ExtraFilesProxyUsername` and `ExtraFilesProxyPassword`."	Sophos Anti-Virusfailed to download `ExtraFiles`. No action required unless this message is repeated. If it fails repeatedly check: `ExtraFilesProxyUsername` and `ExtraFilesProxyPassword` are correct.	`BAD-EXTRAFILES-PROXY-AUTHENTICATION`

Syslog Message	Description	Message ID
"Failed to download '%s': no such file. Please check `ExtraFilesSourcePath`."	Sophos Anti-Virusfailed to download `ExtraFiles`. No action required unless this message is repeated. If it fails repeatedly check: `ExtraFilesSourcePath` is correct.	`BAD-EXTRAFILES-URL`
"Failed to download '%s': invalid authentication. Please check `PrimaryUpdateUsername` and `PrimaryUpdatePassword`."	Sophos Anti-Virus can't authenticate to the primary update source. No action required unless this message is repeated. If it fails repeatedly check: `PrimaryUpdateUsername` and `PrimaryUpdatePassword`. are correct.	`BAD-PRIMARY-AUTHENTICATION`

"Failed to download '%s': invalid proxy authentication.
Please check
`PrimaryUpdate`
`ProxyUsername` and
`PrimaryUpdate`
`ProxyPassword`."
	Sophos Anti-Virus can't authenticate to the primary source proxy.
	No action required unless this message is repeated. If it fails repeatedly check:
	Check
	`PrimaryUpdate`
	`ProxyUsername`
	and `PrimaryUpdate`
	`ProxyPassword`
	are correct.
		`BAD-PRIMARY-PROXY-AUTHENTICATION`

"Failed to download '%s': no such file. Please check `PrimaryUpdateSourcePath`."	Sophos Anti-Virus can't reach the primary update source. No action required unless this message is repeated. If it fails repeatedly check: Check `PrimaryUpdateSourcePath` is correct.	`BAD-PRIMARY-URL`

Syslog Message	Description	Message ID
"Failed to download '%s': invalid authentication. Please check SecondaryUpdateUsername and SecondaryUpdatePassword."	Sophos Anti-Virus can't authenticate to the secondary update source. No action required unless this message is repeated. If it fails repeatedly check: SecondaryUpdateUsername and SecondaryUpdatePassword. are correct.	BAD-SECONDARY-AUTHENTICATION
"Failed to download '%s': invalid proxy authentication. Please check SecondaryUpdate ProxyUsername and SecondaryUpdate ProxyPassword."	Sophos Anti-Virus can't authenticate to the primary source proxy. No action required unless this message is repeated. If it fails repeatedly check: Check SecondaryUpdate ProxyUsername and SecondaryUpdate ProxyPassword are correct.	BAD-SECONDARY-PROXY-AUTHENTICATION
"Failed to download '%s': no such file. Please check SecondaryUpdate SourcePath."	Sophos Anti-Virus can't reach the primary update source. No action required unless this message is repeated. If it fails repeatedly check: Check SecondaryUpdate SourcePath. is correct.	BAD-SECONDARY-URL
"Failed to find validation certificate at %s"	Sophos Anti-Virus didn't update due to the missing verification certificate. If this message repeats uninstall and reinstall Sophos Anti-Virus.	CERTIFICATE_NOT_FOUND
"Timeout connecting to server %s"	Savupdate timed out while trying to connect to an update server at the specified address.	CONNECTION-TIMEOUT

Syslog Message	Description	Message ID
"Savupdate control script for 'after upgrade' reported code %s"	Post upgrade custom is failing. Fix or remove the custom script. Sophos Anti-Virus has been updated.	`CONTROL_SCRIPT` `_AFTER_UPGRADE_ABORT`
"Savupdate control script for 'before upgrade' aborted upgrade with code %s"	Pre upgrade custom is failing. Fix or remove the custom script. Sophos Anti-Virus has not been updated.	`CONTROL_SCRIPT_` `BEFORE_UPGRADE_ABORT`
"Failed to replicate from %s."	Sophos Anti-Virus didn't update. No action required unless this message is repeated. If update fails repeatedly check update settings.	`FAILED-TO-UPDATE-FROM`
"Failed to verify a manifest file '%s'."	Sophos Anti-Virus didn't update. No action required unless this message is repeated. If update fails repeatedly: If updating from CID rebuild the source. If updating from Sophos reinstall Sophos Anti-Virus.	`FAILED_VERIFY_MANIFEST`
"Update failed: Invalid checksum for %s from %s."	Sophos Anti-Virus didn't update. No action required unless this message is repeated. If update fails repeatedly: If updating from CID rebuild the source. If updating from Sophos reinstall Sophos Anti-Virus.	`INVALID-CHECKSUM-FROM`
"Failed to validate contents of cache directory '%s'."	Sophos Anti-Virus didn't update. No action required unless this message is repeated. If update fails repeatedly: If updating from CID rebuild the source. If updating from Sophos reinstall Sophos Anti-Virus.	`MSG_COMPOUNDSINK` `_VALIDATE_FAIL`

Syslog Message	Description	Message ID
"Failed to update Sophos Anti-Virus ."	Sophos Anti-Virus didn't update. No action required unless this message is repeated. If update fails repeatedly check the other log messages to find appropriate action.	`MSG_RTC_UPDATE_FAIL`
"Failed to update - no valid configuration found."	Sophos Anti-Virus can't update. No action required unless this message is repeated. If update fails repeatedly check the update settings.	`NO_VALID` `_CONFIGURATION_FOUND`
"Failed to update from primary update source. Redirecting to secondary update source."	Sophos Anti-Virus updated from the secondary settings, as primary settings failed. Check the primary update settings and the primary servera availability.	`SECONDARY-REPORT-AS-ERROR`
"Updated to versions - SAV: %s[Engine: %s[Data: %s]"	Sophos Anti-Virus updated. No action required.	`UPDATED_TO_VERSION %s %s %s`
"Failed to find suitable product in warehouse at %s."	Sophos Anti-Virus didn't update. No action required unless this message is repeated. If update fails repeatedly please reinstall Sophos Anti-Virus.	`UPDATE_FAILURE` `_PRODUCT_UNAVAILABLE`
"Warehouse certificate chain is invalid. The update source address is %s."	Sophos Anti-Virus didn't update. No action required unless this message is repeated. If update fails repeatedly please reinstall Sophos Anti-Virus.	`UPDATE_FAILURE_SDDS` `_BAD_CERTIFICATE_CHAIN`
"Failed to validate warehouse signatures. The update source address is %s."	Sophos Anti-Virus didn't update. No action required unless this message is repeated. If update fails repeatedly please reinstall Sophos Anti-Virus.	`UPDATE_FAILURE_SDDS` `_SIGNING_ERROR`
"Failed to find supplement warehouse. The update source address is %s."	Sophos Anti-Virus didn't update. It can't find the supplement warehouse. Check the settings.	`UPDATE_FAILURE_SUPPLEMENT` `_WAREHOUSE_UNAVAILABLE`
"Updating from versions - SAV: %s[Engine: %s[Data: %s]."	Sophos Anti-Virus is updating. No action required.	`UPDATING_FROM_VERSION`

Syslog Message	Description	Message ID
"Main configuration is not available[using backup configuration."	Sophos Anti-Virusupdated from the backup settings. Please ensure that the primary update settings are configured correctly.	`USING_BACKUP` `_CONFIGURATION`
"Unable to use %s policy. Using %s policy instead."	Sophos Anti-Virus is configured to update from a SDDS Tag that isn't available in your warehouse. Please ensure that `PrimaryUpdatePolicy` is set correctly.	`Unable to follow %s policy[following %s instead`
"Failed to validate contents of package directory '%s'."	Sophos Anti-Virus didn't update. No action required unless this message is repeated. If update fails repeatedly please reinstall Sophos Anti-Virus.	`VERIFICATION_FAILED`
"Unable to locate signature verifier at %s."	Sophos Anti-Virus didn't update. No action required unless this message is repeated. If update fails repeatedly please reinstall Sophos Anti-Virus.	`VERSIG_MISSING`
"magent (%s) unexpectedly terminated with signal: %s."	magent died due to a signal. sophosmgmtd will automatically restart magent. No action required unless this message is repeated. If message repeats please contact Sophos Support.	`MAGENT-DIED-SIGNAL`
"magent (%s) exited with an error (%s)."	magent exited unexpectedly. sophosmgmtd will automatically restart magent. No action required unless this message is repeated. If message repeats please contact Sophos Support.	`MAGENT-EXIT-ERROR`
"mrouter (%s) unexpectedly terminated with signal: %s."	mrouter died due to a signal. sophosmgmtd will automatically restart mrouter. No action required unless this message is repeated. If message repeats please contact Sophos Support.	`MROUTER-DIED-SIGNAL`

Syslog Message	Description	Message ID
"mrouter (%s) exited with an error (%s)."	mrouter exited unexpectedly. sophosmgmtd will automatically restart mrouter. No action required unless this message is repeated. If message repeats please contact Sophos Support.	`MROUTER-EXIT-ERROR`

Info messages

These messages give you information about the scanning process.

Syslog Message	Description	Message ID
"Sophos Anti-Virus daemon started."	Sophos Anti-Virus started.	`SAVD-STARTED`
"Sophos Anti-Virus daemon stopped."	Sophos Anti-Virus stopped.	`SAVD-STOPPED`
"Loading SAV Interface returned the error %s : %s."	The Sophos Anti-Virus interface did not open due to an error.	`SAVI_LOAD_ERROR`
"scan processor running."	The Sophos Anti-Virus scanner is running.	`SCANNER-RUNNING`
"scan processor stopped."	The Sophos Anti-Virus scanner stopped.	`SCANNER-SHUTDOWN`
"Shut down a scan processor with a signal: %s."	savscand died due to a signal. sophosmgmtd will automatically restart savscand. No action required unless this message is repeated. If message repeats please contact Sophos Support.	`SCANNER-SHUTDOWN-WITH-SIGNAL`
"Failed to disinfect %s: too many disinfection attempts."	Sophos Anti-Virus ondemand scanner didn't disinfect a file. Please remove this file.	`NOTIFY-ONDEMAND-MAX-DISINFECT-ERROR`
"Failed to open %s."	Sophos Anti-Virus ondemand scanner can't open a file. This can happen where the files that the scanner can't open , such as network files. Note that such files haven't been scanned.	`NOTIFY-ONDEMAND-OPEN-ERROR`

Syslog Message	Description	Message ID
"Failed to scan specified path %s."	Sophos Anti-Virusscheduled scan wasn't able to scan an explicitly requested path, Please ensure that the scheduled scan configuration is correct.	`NOTIFY-ONDEMAND-SPECIFIED-PATH-ERROR`
"On-demand scan details: master boot records scanned: %s[boot records scanned: %s[files scanned: %s[scan errors: %s[threats detected: %s, infected files detected: %s."	Sophos Anti-Virus completed an on-demand scan. These are the summary results.	`SAVSCAN-DETAILS`
"On-demand scan finished."	Sophos Anti-Virus on demand scan finished.	`SAVSCAN-FINISHED`
"On-demand scan started."	Sophos Anti-Virus on demand scan started.	`SAVSCAN-START`
" Scheduled scan \"%s\" started."	Sophos Anti-Virus scheduled scan started.	`SCHEDULED-SCAN-BEGIN`
" Scheduled scan \"%s\" completed: master boot records scanned: %s[boot records scanned: %s[files scanned: %s[scan errors: %s[threats detected: %s, infected files detected: %s."	Sophos Anti-Virus completed a scheduled scan. These are the summary results.	`SCHEDULED-SCAN-DETAILS`
"Successfully updated Sophos Anti-Virus from %s"	Sophos Anti-Virus successfully updated.	`SUCCESSFULLY_` `UPDATED_FROM`

14 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.

14.1 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.

14.2 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
```

14.3 Check the auto-updating configuration for a computer

1. At the computer that you want to check, type:
   `/opt/sophos-av/bin/savsetup`
   `savsetup` asks you to select what you want to do.
2. Select **Display update configuration** to see the current configuration.

14.4 Configure multiple update clients to update from Sophos directly when the update server is unavailable

> **Note**
> If you want to change the configuration for a single update client, see Configure a single update client to update from the update server (page 42) instead.

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

To configure multiple update clients to update from Sophos directly when the update server is unavailable:

1. Set the secondary update source address to `sophos:`, using the parameter SecondaryUpdateSourcePath . For example, type:
   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file -c set
   SecondaryUpdateSourcePath 'sophos:'
   ```
2. Set the secondary update source username to the username that is included with your license, using the parameter SecondaryUpdateUsername. For example, type:
   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file -c set
   SecondaryUpdateUsername 'cust123'
   ```
3. Set the secondary update source password to the password that is included with your license, using the parameter SecondaryUpdatePassword. For example, type:
   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file -c set
   SecondaryUpdatePassword 'j23rjjfwj'
   ```
4. If you access the internet via a proxy, set the address, username, and password of the proxy server, using the parameters SecondaryUpdateProxyAddress, SecondaryUpdateProxyUsername, and SecondaryUpdateProxyPassword, respectively. For example, type:
   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file -c set
   SecondaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'
   /opt/sophos-av/bin/savconfig -f offline-config-file -c set
   SecondaryUpdateProxyUsername 'penelope'
   /opt/sophos-av/bin/savconfig -f offline-config-file -c set
   SecondaryUpdateProxyPassword 'fj202jrjf'
   ```
5. 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
```

For example:

```
/opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /opt/sophos-av/extrafiles/LiveConfig.cfg
```

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

Note

If you want to change the configuration for multiple update clients, see Configure multiple update clients to update from Sophos directly when the update server is unavailable (page 41) instead.

1. At the computer that you want to configure, type:
   `/opt/sophos-av/bin/savsetup`
   `savsetup` asks you to select what you want to do.
2. Select the option to configure the primary (or secondary) update source to be your own server.
   `savsetup` prompts you to enter details of the update source.
3. Enter the address of the source, and the username and password if required.

   You can specify either an HTTP address or a UNC path, depending on how you have set up the update server.

   `savsetup` asks you if you need a proxy to access the update server.
4. If you need a proxy, press Y and then type the proxy details.

15 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
```

16 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 14).

16.1 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.

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

Symptom

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

Cause

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

Resolve the problem

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

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

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

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

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

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

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

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

   where *values* are the existing settings.
4. Save the login script or profile.

16.3 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.

16.4 On-demand scanning runs slowly

This problem may arise for one of the following reasons:

Symptom

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

Causes

This might be for one of the following reasons:

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

Resolve the problem

Try one of the following, as appropriate:

- Avoid using full scanning unless you are advised to, for example by Sophos technical support.
- To scan files that have specific filename extensions, add those extensions to the list of file types that Sophos Anti-Virus scans by default. For more information, see Scan a particular directory or file (page 4).

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

Symptom

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

Cause

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

Resolve the problem

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

16.6 Virus not cleaned up

Symptoms

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

Causes

This might be for one of the following reasons:

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

Resolve the problem

Try one of the following, as appropriate:

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

16.7 Virus fragment reported

Symptom

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

Causes

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

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

Resolve the problem

1. Update Sophos Anti-Virus on the affected computer so that it has the latest virus data.
2. Try to disinfect the file: see Disinfect a specific infected file (page 10).
3. If virus fragments are still reported, contact Sophos technical support for advice.

17 Glossary

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-demand scan

A scan that you initiate. You can use an on-demand scan to scan anything from a single file to everything on your computer that you have permission to read.

primary update source

The location of the updates that a computer usually accesses. It might need access credentials.

scheduled scan

A scan of your computer, or parts of your computer, that runs at set times.

secondary update source

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

update client

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

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.

18 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.

19 Legal notices

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

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

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™ (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (c) 1993-2014, all rights reserved. Since DOC software is open-source, freely available software, you are free to use, modify, copy, and distribute —perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with any code built using DOC software that you release. No copyright statement needs to be provided if you just ship binary executables of your software products.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not misappropriate the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, in a way that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us know so we can promote your project in the DOC software success stories.

The ACE, TAO, CIAO, DAnCE, and CoSMIC web sites are maintained by the DOC Group at the Institute for Software Integrated Systems (ISIS) and the Center for Distributed Object Computing of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter "as is" with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

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

curl

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

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 © 1998–2016 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

A

alerts
- command-line 8
- desktop pop-up 8
- email 25

analyses of viruses 9
archives
- on-demand scans 5, 5

B

backups of scanned files 46

C

cleaning up infected files 10
cleanup information 9
CLI (command-line interface) 2
command-line alerts 8
command-line interface (CLI) 2
configuring Sophos Anti-Virus 2

D

deleting infected files 11, 11
desktop pop-up alerts 8
directories, on-demand scans 4, 5
disinfecting
- infected files 10, 10

disk space insufficient 45

E

email alerts 25
Enterprise Console 2
error codes 14
excluding items
- on-demand scans 6

F

file types, on-demand scans 5, 7
files, on-demand scans 4, 5
filesystems, on-demand scans 4, 6
fragment reported, viruses 47

I

infected files
- cleaning up 10
- deleting 11, 11
- disinfecting 10, 10
- quarantining 9

L

layers, in configuration file 18
log, Sophos Anti-Virus
- configuring 27
- viewing 12, 24

log[syslog 28

M

man page not found 44

N

No manual entry for ... 44

O

on-demand scans
- archives 5, 5
- directories 4, 5
- excluding items 6
- file types 5, 7
- files 4, 5
- filesystems 4, 6
- remote computers 6
- scheduled scans 21
- symbolically linked items 6
- UNIX executables 7

Q

quarantining infected files 9

R

remote computers, on-demand scans 6
return codes 14

S

savconfig 19
savsetup 40
scheduled scans 21
side-effects of viruses 11
slow on-demand scans 45
Sophos Anti-Virus log
- configuring 27
- viewing 12, 24

symbolically linked items, on-demand scans 6
syslog 28

U

UNIX executables, on-demand scans 7

updating
- configuring 40
- immediate 13

V

viruses
- analyses 9
- detected 8, 26
- fragment reported 47
- not cleaned up 47
- side-effects 11