

SOPHOS

Sophos Anti-Virus for UNIX and Linux startup guide

Product version: 4

Document date: January 2011



Contents

1 About this guide.....	3
2 System requirements.....	4
3 About Sophos Anti-Virus for UNIX and Linux.....	5
4 Installing Sophos Anti-Virus on a standalone computer.....	6
5 Run an on-demand scan of the computer.....	9
6 What happens if viruses are detected.....	10
7 Updating Sophos Anti-Virus.....	11
8 Remove Sophos Anti-Virus.....	14
9 Appendix: Install Sophos Anti-Virus on networked computers.....	15
10 Technical support.....	16
11 Legal notices.....	17

1 About this guide

This guide tells you how to install Sophos Anti-Virus on standalone and networked UNIX and Linux computers.

You can find details of all configuration options in the man pages and the *Sophos Anti-Virus for UNIX and Linux user manual* for version 4.

To install Sophos Anti-Virus so that it is updated automatically by Sophos Enterprise Console, see the *Sophos Endpoint Security and Control startup guide for Linux, NetWare, and UNIX* instead of this guide.

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

2 System requirements

For system requirements, go to the system requirements page of the Sophos website (<http://www.sophos.com/products/all-sysreqs.html>).

3 About Sophos Anti-Virus for UNIX and Linux

3.1 What Sophos Anti-Virus does

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

3.2 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.

4 Installing Sophos Anti-Virus on a standalone computer

4.1 Download Sophos Anti-Virus

1. Log in to <http://www.sophos.com/support/updates/> with your MySophos username and password.
2. On the web page for Endpoint Security and Data Protection downloads, click the appropriate link for your system:
 - For UNIX, click the link for anti-virus for UNIX and NetWare.
 - For Linux, click the link for anti-virus for Linux.
3. On the web page that is displayed, download the Sophos Anti-Virus version 4 tarball for your platform to a temporary directory, for example /tmp.

If you have a version of FreeBSD 5 earlier than 5.2, you may need to install the version 4 binary compatibility libraries. Similarly, if you have a version of FreeBSD 4 earlier than 4.5, you may need to install the version 3 binary compatibility libraries. To check which version of FreeBSD you have, type:

```
uname -v
```

There are two Linux on Intel tarballs. If you have a Linux libc6 system with glibc 2.2 or later, you can use the glibc 2.2 tarball. It provides new features, for example large file support and improved multi-threading capabilities. Note that the latter feature requires that /lib contains the libpthread.so library. If you have a very old Linux libc6 system, use the standard libc6 tarball. However, Sophos Anti-Virus might not work with versions of glibc that are earlier than 2.1. To check which version of glibc you have, look in /lib at the libc6 library file. On some systems, this is a symbolic link to a filename in the form libc-2.2.*so, from which the version is apparent.

4.2 Extract the installation files

1. Change to the temporary directory to which you downloaded the Sophos Anti-Virus tarball.
2. Untar the tarball to the temporary directory:

```
tar -xzf tarball
```

where *tarball* is the tarball filename.

A directory sav-install is created in the temporary directory, which contains the extracted installation files.

4.3 Run the installation script

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

1. Change to the directory sav-install.
2. Run the installation script:

./install.sh

A warning about the environment variable MANPATH might be displayed. You can safely ignore this warning, as the installation is performed correctly.

By default, the script copies:

- The **sweep** program to /usr/local/bin.
- The shared library to /usr/local/lib.
- Virus data to /usr/local/sav.
- The manual page to /usr/local/man.

Note: You can specify the files that are installed and the directories to which they're installed by running the script with various options. For more information, run the script with the option **-h**.

4.4 Check environment variables

You need to ensure that your system's environment variables include the directories that Sophos Anti-Virus uses.

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 variables include the directories that Sophos Anti-Virus uses:

PATH should include /usr/local/bin

MANPATH should include /usr/local/man

LD_LIBRARY_PATH should include /usr/local/lib

Note: On AIX, the library environment variable is LIBPATH, and on HP-UX it is SHLIB_PATH.

3. If the environment variables do not include these directories, add them as follows. Do not change any of the existing settings.

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

```
PATH=$PATH:/usr/local/bin
export PATH
MANPATH=$MANPATH:/usr/local/man
export MANPATH
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib
export LD_LIBRARY_PATH
```

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

```
setenv PATH values:/usr/local/bin
setenv MANPATH values:/usr/local/man
setenv LD_LIBRARY_PATH values:/usr/local/lib
```

where *values* are the existing settings.

Note: On some systems, for example FreeBSD and Linux, you can enable Sophos Anti-Virus to use the Sophos Anti-Virus shared libraries by running **ldconfig**. This might require editing of `/etc/ld.so.conf`.

4. Save the login script or profile.

4.5 Add the latest virus data

To detect viruses that have been discovered since your version of Sophos Anti-Virus was compiled, you must add the latest virus data. This is in the form of *IDE files*. An IDE file is a file that enables Sophos Anti-Virus to detect and disinfect a particular virus.

1. Go to <http://www.sophos.com/downloads/ide/>.
2. Download the compressed IDEs file for your version of Sophos Anti-Virus.
3. Extract the IDEs to the directory `/usr/local/sav`.

Note: If you specified a different directory for virus data when you ran the installation script, you must extract the IDEs to that directory instead.

5 Run an on-demand scan of the computer

Having just installed Sophos Anti-Virus, we recommend that you scan the whole computer for viruses, especially if it's a server and you want to minimize the possibility of spreading viruses to the other computers. To do this, you run an *on-demand scan*.

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

6 What happens if viruses are detected

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:

```
SWEEP virus detection utility
Version 4.58.0 [Linux/Intel]
Virus data version 4.58, October 2010
Includes detection for 1375239 viruses, Trojans and worms
Copyright (c) 1989-2010 Sophos Group. All rights reserved.

System time 13:43:32, System date 22 September 2010

IDE directory is: /usr/savides/

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 Sweep.
```

For information about cleaning up viruses, see the *Sophos Anti-Virus for UNIX and Linux user manual* for version 4.

7 Updating Sophos Anti-Virus

To enable Sophos Anti-Virus to detect all the latest viruses, you must update it:

- Each month, when we release the new version of Sophos Anti-Virus.
- When a significant new virus emerges.

7.1 Updating Sophos Anti-Virus each month

Sophos releases a new version of Sophos Anti-Virus each month, according to the schedule on http://www.sophos.com/downloads/release_dates/.

7.1.1 Clear old virus data

- Delete all *.ide files from the directory /usr/local/sav.

Note: If you specified a different directory for virus data when you ran the installation script, you must delete the *.ide files from that directory instead.

7.1.2 Download Sophos Anti-Virus

1. Log in to <http://www.sophos.com/support/updates/> with your MySophos username and password.
2. On the web page for Endpoint Security and Data Protection downloads, click the appropriate link for your system:
 - For UNIX, click the link for anti-virus for UNIX and NetWare.
 - For Linux, click the link for anti-virus for Linux.

3. On the web page that is displayed, download the Sophos Anti-Virus version 4 tarball for your platform to a temporary directory, for example /tmp.

If you have a version of FreeBSD 5 earlier than 5.2, you may need to install the version 4 binary compatibility libraries. Similarly, if you have a version of FreeBSD 4 earlier than 4.5, you may need to install the version 3 binary compatibility libraries. To check which version of FreeBSD you have, type:

```
uname -v
```

There are two Linux on Intel tarballs. If you have a Linux libc6 system with glibc 2.2 or later, you can use the glibc 2.2 tarball. It provides new features, for example large file support and improved multi-threading capabilities. Note that the latter feature requires that /lib contains the libpthread.so library. If you have a very old Linux libc6 system, use the standard libc6 tarball. However, Sophos Anti-Virus might not work with versions of glibc that are earlier than 2.1. To check which version of glibc you have, look in /lib at the libc6 library file. On some systems, this is a symbolic link to a filename in the form libc-2.2.*so, from which the version is apparent.

7.1.3 Extract the installation files

1. Change to the temporary directory to which you downloaded the Sophos Anti-Virus tarball.
2. Untar the tarball to the temporary directory:

```
tar -xzf tarball
```

where *tarball* is the tarball filename.

A directory sav-install is created in the temporary directory, which contains the extracted installation files.

7.1.4 Run the installation script

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

1. Change to the directory sav-install.

2. Run the installation script:

./install.sh

A warning about the environment variable MANPATH might be displayed. You can safely ignore this warning, as the installation is performed correctly.

By default, the script copies:

- The **sweep** program to /usr/local/bin.
- The shared library to /usr/local/lib.
- Virus data to /usr/local/sav.
- The manual page to /usr/local/man.

Note: You can specify the files that are installed and the directories to which they're installed by running the script with various options. For more information, run the script with the option **-h**.

7.1.5 Add the latest virus data

To detect viruses that have been discovered since your version of Sophos Anti-Virus was compiled, you must add the latest virus data. This is in the form of *IDE files*. An IDE file is a file that enables Sophos Anti-Virus to detect and disinfect a particular virus.

1. Go to <http://www.sophos.com/downloads/ide/>.
2. Download the compressed IDEs file for your version of Sophos Anti-Virus.
3. Extract the IDEs to the directory /usr/local/sav.

Note: If you specified a different directory for virus data when you ran the installation script, you must extract the IDEs to that directory instead.

7.2 Update Sophos Anti-Virus when a significant new virus emerges

You can receive email notifications about new viruses by registering at <https://secure.sophos.com/security/notifications>.

To update Sophos Anti-Virus when a significant new virus emerges:

1. Go to <http://www.sophos.com/downloads/ide/>.
2. Download the compressed IDEs file for your version of Sophos Anti-Virus.
3. Extract the IDEs to the directory /usr/local/sav.

Note: If you specified a different directory for virus data when you ran the installation script, you must extract the IDEs to that directory instead.

8 Remove Sophos Anti-Virus

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

All directories below refer to the installation defaults. If you specified different directories when you ran the installation script, you must apply these instructions to those directories instead.

1. Delete the **sweep** program: `/usr/local/bin/sweep`.
2. Delete the shared library: `/usr/local/lib/libsavi.*`.
3. Delete the virus data directory: `/usr/local/sav`.
4. Delete the configuration file: `/etc/sav.conf`.
5. Delete the manual page: `/usr/local/man/man1/sweep.1`.

Note: On SCO systems, delete `/usr/local/man/man.1/sweep.1` instead.

9 Appendix: Install Sophos Anti-Virus on networked computers

This procedure assumes that there is a trust relationship between the computers.

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

If you have multiple, networked UNIX or Linux computers, you may want to install and update Sophos Anti-Virus from a central directory, rather than carrying out installation at each computer separately.

To install Sophos Anti-Virus on networked computers:

1. On one of the computers, create a directory that is accessible by all the other computers.
2. Download Sophos Anti-Virus to this directory, by following the steps in [Download Sophos Anti-Virus](#) (page 11).
Repeat these steps for all the different platforms on your network.
3. Extract the installation files to this directory, by following the steps in [Extract the installation files](#) (page 12).

If you have more than one platform on your network, extract the files into separate subdirectories.

4. Change to the directory sav-install.
5. Use **ssh** to run the installation script on each computer from the shared directory:
ssh -l username hostname / .install.sh

where *username* is your user ID and *hostname* is the name of the computer on which you want to install Sophos Anti-Virus. You can put this command into a script to install Sophos Anti-Virus on all computers that share the same platform.

Note: You can specify the files that are installed and the directories to which they're installed by running the script with various options. For more information, run the script with the option **-h**.

If you have more than one platform on your network, ensure that you run the installation script from the correct set of installation files for each platform.

On older UNIX systems, **ssh** might not be available. You can use **rsh** instead, although it is less secure.

6. If you want to check the environment variables on each computer, follow the steps in [Check environment variables](#) (page 7) for each computer.
7. If you want to ensure each computer is able to detect viruses that have been discovered since your version of Sophos Anti-Virus was compiled, follow the steps in [Add the latest virus data](#) (page 13) for each computer.

10 Technical support

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

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

11 Legal notices

Copyright © 2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

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