SOPHOS

sophos anti-virus

Startup guide

UNIX

Document date: April 2006

About this guide

This guide tells you how to do the following on a single UNIX computer:

- install Sophos Anti-Virus
- add the latest virus identities
- scan the computer for viruses
- eliminate viruses
- update Sophos Anti-Virus
- remove Sophos Anti-Virus.

It also tells you how to

- install Sophos Anti-Virus on multiple UNIX computers
- set up central reporting from non-UNIX workstations
- specify non-default installation options.

You can find details of all other configuration options in the *Sophos Anti-Virus UNIX user manual* on the Sophos website or the **Sophos Anti-Virus Supplementary CD**.

If you want to install and update Sophos Anti-Virus automatically using EM Library, refer to the *Sophos Anti-Virus and Sophos Client Firewall network startup guide* on the Sophos website or the **Sophos Network Install CD**.

Contents

1 Installing Sophos Anti-Virus

If you have multiple, networked UNIX computers, and you want to install and update Sophos Anti-Virus from a central directory, rather than carrying out installation at each computer separately, go to appendix 1.

InterCheck Server is a daemon that runs on a UNIX server, and processes virus alerts sent from Windows, Macintosh and OS/2 workstations. It is not vital to the running and updating of Sophos Anti-Virus. To use it you need to set up a user and group for the daemon and set permissions on a common directory. Refer to appendix 2.

There are three steps in the Sophos Anti-Virus installation process:

- Extract the installation files (section 1.1).
- Install Sophos Anti-Virus (section 1.2).
- Check your system settings (section 1.3).

1.1 Extracting the installation files

Extract the installation files from the **Sophos Anti-Virus Supplementary CD** as follows.

1. Log on to the computer with root privileges, and insert the **Sophos Anti-Virus Supplementary CD**.
2. Mount the **Sophos Anti-Virus Supplementary CD** and list the contents of the `unix` subdirectory.
3. Select the archive file for your version of UNIX.

   For Linux on Intel users:

   If you have a newer libc6 system with glibc 2.2 or later, such as RedHat 7 or later, you need

   `linux.intel.libc6.glibc.2.2.tar`

   If you have an older libc6 system, such as RedHat 6, SUSE 6, or Slackware 7, you need

   `linux.intel.libc6.tar`

To check which kind of system you have, look in the `/lib` directory for a file or link called `libc.so.6` or similar. Presence of the file indicates a libc6 system.

4. Copy the appropriate archive file to the `/tmp` directory.
5. Untar the archive file into `/tmp` as follows

   ```
   cd /tmp
   tar xvf linux.intel.libc6.glibc.2.2.tar
   ```

   or

   ```
   cd /tmp
   tar xvf linux.intel.libc6.tar
   ```

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

   Now install Sophos Anti-Virus (section 1.2).

1.2 Installing Sophos Anti-Virus

To install Sophos Anti-Virus ***without*** InterCheck Server (recommended), run the installation script as follows:

```
cd sav-install
./install.sh
```

To install Sophos Anti-Virus ***with*** InterCheck Server, run the installation script with the `-i` option (you must have already followed the instructions in appendix 2.1):

```
cd sav-install
./install.sh -i
```

For information on all the options with which you can run the installation script, see appendix 3.

You may now see a warning about the `MANPATH` environment variable. However, the installation will be made correctly.

The installation script places

- binaries in `/usr/local/bin`
- shared library in `/usr/local/lib`
- virus data in `/usr/local/sav`
- manual pages in `/usr/local/man`

Now check your system settings (section 1.3).

1.3 Checking system settings

Ensure that the environment variables in your login script or profile include the directories that Sophos Anti-Virus uses.

`PATH` should include `/usr/local/bin`

`MANPATH` should include `/usr/local/man`

If any of these variables are not included, add them to the environment variable(s) as in the examples below. Do not alter any of the existing settings.

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

```
PATH=$PATH:/usr/local/bin
export PATH
```

If you are running the csh or tcsh shell, enter

```
setenv PATH <values>:/usr/local/bin
```

where `<values>` are the existing settings.

If more than one user is going to run Sophos Anti-Virus, you need to make these variables system-wide. To do this, amend `/etc/login` or `/etc/profile`.

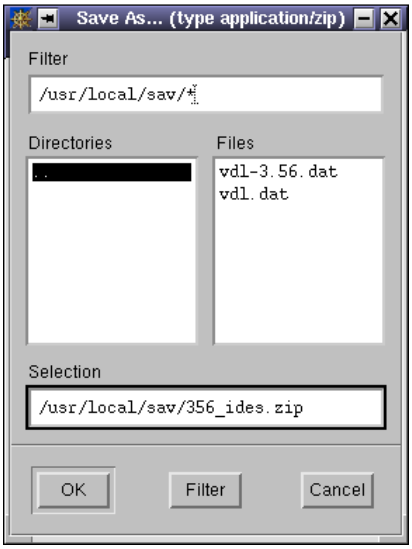
If you do not have a login script, you will need to reset the values each time you start the computer.

Now add the latest virus identity files (IDEs) to the computer (section 2).

2 Adding the latest virus identity files (IDEs)

A **virus identity file (IDE)** is a file that enables Sophos Anti-Virus to detect a specific virus. You need IDEs to protect your computer against viruses discovered since your version of Sophos Anti-Virus was compiled.

1. Go to the IDE download page of the Sophos website (www.sophos.com/downloads/ide).
2. Download the compressed IDEs file for your version of Sophos Anti-Virus.
3. Extract the IDE files to the `usr/local/sav` directory.



If you prefer, scroll down the page and download the IDEs one by one, to the location above.

Help with downloading IDEs is available in the Sophos support knowledgebase (www.sophos.com/support/knowledgebase). If you use Internet Explorer 5.0, read the article on why IDEs may acquire an extra file extension when you download them.

If you need further help with downloading IDEs, please contact Sophos technical support.

Sophos Anti-Virus is now installed and up to date on the computer.

If you are *installing* Sophos Anti-Virus with central reporting, you now activate InterCheck Server (appendix 2.2). If you are *updating* Sophos Anti-Virus with central reporting, you have finished the update.

For more information see the following sections of this guide:

- Section 3 describes how to scan the computer for viruses.
- Section 4 describes how to eliminate viruses.
- Section 5 describes how to update Sophos Anti-Virus.
- Section 6 describes how to remove Sophos Anti-Virus.

3 Scanning the computer for viruses

To scan the local machine, enter

```
sweep /
```

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

```
sweep /usr/mydirectory/myfile
```

After the scan, you will see a message similar to that shown below.

If Sophos Anti-Virus has found a virus, it reports it in the line which starts with `>>>` followed by either `Virus` or `Virus Fragment`:

```
SWEEP virus detection utility
Version 3.90.0 [Linux/Intel]
Virus data version 3.90, February 2005
Includes detection for 99603 viruses, trojans and worms
Copyright (c) 1989-2005 Sophos Plc, www.sophos.com

System time 09:35:55, System date 16 February 2005

Quick Sweeping

>>> Virus 'EICAR-AV-Test' found in file /home/source/eicar.src

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

For help using Sophos Anti-Virus, enter

```
sweep -h
```

4 Eliminating viruses

The method you use to eliminate a virus with Sophos Anti-Virus depends on whether the infected object is a data file (e.g. a document or a spreadsheet) or a program.

4.1 To eliminate a virus from a data file

To eliminate a virus from a specific data file, enter

```
sweep <object> -di
```

where `<object>` is the path to the infected data file.

Alternatively, to detect and remove viruses from any data file on the computer, enter

```
sweep / -di
```

In either case, Sophos Anti-Virus asks you for confirmation before it removes the virus(es).

! Check the data file(s) carefully afterwards. Sophos Anti-Virus can remove the virus, but cannot reverse any side-effects. Check the analysis of the virus on the Sophos website for more information.

4.2 To eliminate a virus from a program

To eliminate a virus from a program, remove the program and replace it from a backup or from the original disk.

To remove a specific infected program, enter

```
sweep <object> -remove
```

where `<object>` is the infected program.

Alternatively, to detect and remove any infected programs on the system, enter

```
sweep / -remove
```

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

5 Keeping Sophos Anti-Virus up to date

You must update Sophos Anti-Virus regularly to enable it to detect all the latest viruses. Do this

- each month, when the new version of Sophos Anti-Virus is released (section 5.1)
- whenever a significant new virus that puts your computer at risk is released (section 5.2).

5.1 To update Sophos Anti-Virus each month

A new version of Sophos Anti-Virus is released each month. To find out when, go to the Sophos Anti-Virus release dates page of the Sophos website (www.sophos.com/downloads/release_dates/).

Carry out the following steps as soon as the new version is released:

- Download and extract the installation files (section 5.1.1).
- Update Sophos Anti-Virus (section 5.1.2).
- Download the latest compressed IDEs file (section 2).

5.1.1 Download and extract the installation files

Download and extract the installation files from the Sophos website as follows.

1. Delete all *.ide files from `/usr/local/sav`.
2. Log on to the computer with root privileges.

3. Go to the Sophos website product downloads page (www.sophos.com/support/updates). Save the archive file for your version of UNIX to the `/tmp` directory.

   For Linux on Intel users:

   If you have a newer libc6 system with glibc 2.2 or later, such as RedHat 7 or later, you need

   Linux on Intel using libc6 (glibc 2.2)

   If you have an older libc6 system, such as RedHat 6, SUSE 6, or Slackware 7, you need

   Linux on Intel using libc6

To check which kind of system you have, look in the `/lib` directory for a file or link called libc.so.6 or similar. Presence of the file indicates a libc6 system.

4. Uncompress and untar the archive file into `/tmp` as follows

   ```
   cd /tmp
   uncompress  linux.intel.libc6.glibc.2.2.tar.Z
   tar xvf linux.intel.libc6.glibc.2.2.tar
   ```

   or

   ```
   cd /tmp
   uncompress  linux.intel.libc6.tar.Z
   tar xvf linux.intel.libc6.tar
   ```

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

   Now update Sophos Anti-Virus (section 5.1.2).

5.1.2 Update Sophos Anti-Virus

To update Sophos Anti-Virus ***without*** InterCheck Server (recommended), run the installation script as follows:

```
cd sav-install
./install.sh
```

To update Sophos Anti-Virus ***with*** InterCheck Server, run the installation script with the `-i` option:

```
cd sav-install
./install.sh -i
```

For information on all the options with which you can run the installation script, see appendix 3.

You may now see a warning about the `MANPATH` environment variable. However, the update will be made correctly.

The installation script places

- binaries in `/usr/local/bin`
- shared library in `/usr/local/lib`
- virus data in `/usr/local/sav`
- manual pages in `/usr/local/man`

Now download the latest compressed IDEs file (section 2). This will protect your computer against viruses discovered since the new version of Sophos Anti-Virus was released.

5.2 To update whenever a significant new virus is discovered

This type of update is carried out between major monthly updates of Sophos Anti-Virus.

Whenever there is a significant new virus threat that puts your computer at risk, go to the IDE download page of the Sophos website (www.sophos.com/downloads/ide) and download the IDE for the virus to `usr/local/sav`.

To receive email notifications about IDEs and other alerts, register at www.sophos.com/virusinfo/notifications.

6 Removing Sophos Anti-Virus

1. Remove the `sweep` program from `/usr/local/bin`.
2. Remove any Sophos Anti-Virus libraries (`libsavi.*`) from `/usr/local/lib`.
3. Remove the Sophos Anti-Virus data directory `/usr/local/sav` and its contents.
4. Remove the configuration file `/etc/sav.conf`.
5. Remove the manual page `/usr/local/man/man1/sweep.1`.

   Sophos Anti-Virus has been removed from the computer.

Appendices

Installing on multiple UNIX computers

Installing central reporting

Options for non-default installation

Appendix 1 Installing on multiple UNIX computers

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

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

1. On one UNIX computer, set up a shared area that is available to all the other computers.
2. Untar the Sophos Anti-Virus for UNIX distribution archive or archives to this shared area.

   If you have computers on your network that use more than one UNIX operating system (e.g. Linux and FreeBSD), untar the distribution archive for each system into a separate directory.
3. Use ssh to run the install.sh script on every connected UNIX computer, from the shared area. For example, enter

   ```
   ssh -l [username] [hostname] / .install.sh
   ```

   where [username] is your user ID and [hostname] is the computer on which you want to install Sophos Anti-Virus.

   In each case, ensure that you run install.sh from the correct set of distribution files for that computer's operating system.

On older UNIX computers, ssh may not be available. You can use rsh instead, though it is less secure.

Step 3 can be put into a script which is run from one of your UNIX computers.

Appendix 2 Installing central reporting

InterCheck Server is a daemon that runs on a UNIX server, and processes virus alerts sent from Windows, Macintosh and OS/2 workstations. To use it you need to set up a user and group for the daemon and set permissions on a common directory.

To install Sophos Anti-Virus with InterCheck Server, there are six steps:

- Prepare for installation (appendix 2.1).
- Extract the installation files (section 1.1).
- Install Sophos Anti-Virus (section 1.2).
- Check the system settings (section 1.3).
- Add the latest virus identity files (section 2).
- Activate central reporting (appendix 2.2).

Appendix 2.1 Prepare for installation

Before installing Sophos Anti-Virus for UNIX, you must

- create a user group called 'sweep'
- create a user called 'sweep'. The primary group of this user should be 'sweep', and the user should not be allowed to log in at a terminal. You may want to set the shell to `/bin/false`. Check your UNIX documentation for details of how to do this.

Now extract the installation files (section 1.1).

Appendix 2.2 Activate central reporting

To use InterCheck Server, do as follows:

1. Export the `/var/spool/intercheck` directory so that it is visible to the non-UNIX workstations.
2. Start InterCheck Server. Enter

   ```
   icheckd
   ```

   For information on controlling and configuring central reporting, refer to the *Sophos Anti-Virus UNIX user manual*.

Appendix 3 Options for non-default installation

You can specify the Sophos Anti-Virus files that are installed, and the directories where they are installed.

To perform a non-default installation, run the installation script, install.sh, with any of the following options.

-d [prefix]

Installs the programs, library, virus data and manual pages in [prefix]/bin, [prefix]/lib, [prefix]/sav and [prefix]/man.

You do not have to install all these files in the same directory. See the `-b`, `-l`, `-m` and `-s` options.

-b [directory]

Installs the virus scanning programs in [directory].

The other files are installed in the default directory, unless you specify otherwise with the `-l`, `-m` or `-s` options.

-l [directory]

Installs the Sophos Anti-Virus library in [directory].

The other files are installed in the default directory, unless you specify otherwise with the `-b`, `-m` or `-s` options.

-m [directory]

Installs the man pages in [directory].

The other files are installed in the default directory, unless you specify otherwise with the `-b`, `-l` or `-s` options.

-s [directory]

Installs the virus data in [directory].

The other files are installed in the default directory, unless you specify otherwise with the `-b`, `-l` or `-m` options.

-i [directory]

Installs the files for InterCheck Server in [directory]. If no directory is specified, the value in `/etc/icheckd.conf` is used, or the default `/var/spool/intercheck`. The icheckd binary and manual pages are also installed.

-ni

Does not install InterCheck Server at all.

-ssi

Has the same effect as `-i` but also stops and starts InterCheck Server after installation.

-nssi

Does not stop and start InterCheck Server after installation.

-h

Prints help.

-v

Verbose operation. Displays the location of each file as it is installed.

Technical support

For technical support, visit

www.sophos.com/support

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