Symantec™ AntiVirus for Linux 1.0.14 Client Guide

Using Symantec AntiVirus for Linux

This document includes the following topics:

About Symantec AntiVirus for Linux

Symantec AntiVirus for Linux includes real-time antivirus file protection through Auto-Protect scanning and file system scanning. Symantec AntiVirus for Linux provides the following types of protection:

Auto-Protect	Constantly monitors activity on your computer by looking for viruses and security risks in the following situations: ■ When a file is executed or opened. ■ When modifications have been made to a file, such as renaming, saving, moving, or copying a file to and from folders.

Signature-based scanning	Searches for residual virus signatures in infected files, and for the signatures of security risks in infected files and system information. This type of search is called a scan. Your administrator initiates signature-based or pattern-based scans systematically to check the files on your computer for viruses and security risks, such as adware or spyware. An administrator can run scans on demand or schedule them to run unattended.

In the KDE and Gnome desktop environments, your Linux computer displays a yellow shield icon on the status tray. The icon lets you know whether or not your computer is protected. If Symantec AntiVirus is disabled, the icon appears with a black exclamation point next to the shield. If Auto-Protect is disabled, the shield appears with a red circle and a slash through it.

If you do not use a KDE or Gnome desktop environment, you can use the Symantec AntiVirus `sav` command-line interface to see the same information.

What happens when a virus is detected

After a scan detects a virus, Symantec AntiVirus attempts to clean the virus from the infected file and repair the effects of the virus by default. If the file is cleaned, the virus is successfully and completely removed. If Symantec AntiVirus cannot clean the file, Symantec AntiVirus attempts a second action, quarantining the infected file so that the virus cannot spread. Your administrator can also configure Symantec AntiVirus for Linux to delete infected files.

If Symantec AntiVirus for Linux quarantines or deletes a file as the result of an administrator's scan, Symantec AntiVirus does not notify you about it. However, it is possible that an application may display an error message when Symantec AntiVirus denies the application access to the infected file or when the application cannot locate the infected file.

You do not need to take any action when a virus is detected. Your administrator configures Symantec AntiVirus to take appropriate action.

Scanning for security risks is not enabled in Symantec AntiVirus for Linux by default. However, your administrator may enable these scans. If the scan is enabled, the Symantec AntiVirus can detect and log the security risks, but not take any action on them.

Configuration settings and other Symantec AntiVirus for Linux tasks that are available to your administrator are described in the *Symantec AntiVirus for Linux Implementation Guide*.

About updating virus definitions

Every computer that runs Symantec AntiVirus has a copy of the virus and security risks definitions files. These files can become outdated as new risks are discovered. Symantec typically updates definitions files daily, or more frequently if needed. It's important to keep virus and security risks definitions files current to maintain the highest level of protection for your network.

Your administrator may update the definitions on your computer, or may want you to update them yourself by using LiveUpdate. Talk to your administrator to find out whether you should run LiveUpdate yourself.

See "Running LiveUpdate" on page 6.

Displaying status and product information

You can display status and product information by using the user interface or by using command-line interface commands. You can use either method to display the versions of the program, scan engine, and virus definitions that are in use, the status of Auto-Protect, and whether or not a scan is in progress.

If you use a KDE or Gnome environment, you click the yellow shield icon on the status tray.

If you do not use a KDE or Gnome environment, from the command line, you can use the `sav info` command. By default, `sav` is located in the /opt/Symantec/symantec_antivirus directory.

To display status and product information from the user interface

- In the status tray, double-click the yellow shield icon.

To display status and product information from the command line

1. To display the Auto-Protect status, type the following command:

   `/opt/Symantec/symantec_antivirus/sav info -a`

2. To display the virus definitions version, type the following command:

   `/opt/Symantec/symantec_antivirus/sav info -d`

3. To display the current product version, type the following command:

   `/opt/Symantec/symantec_antivirus/sav info -p`

4 To display the current scan engine version, type the following command:

```
/opt/Symantec/symantec_antivirus/sav info -e
```

5 To determine if a scan is in progress, type the following:

```
/opt/Symantec/symantec_antivirus/sav info -s
```

Running LiveUpdate

You can update the virus and security risk definitions on your computer from the user interface or from the command line. You cannot update the definitions if your administrator has configured Symantec AntiVirus to prevent you from running LiveUpdate manually.

To run LiveUpdate from the user interface

1 In the Symantec AntiVirus status window, click **LiveUpdate**.

2 Follow the prompts from the wizard.

To run LiveUpdate from the command line

- From the command line, type the following command:

  ```
  /opt/Symantec/symantec_antivirus/sav liveupdate -u
  ```

  By default, `sav` is located in the `/opt/Symantec/symantec_antivirus` directory.