Symantec™ AntiVirus for Linux 1.0.14 Implementation Guide

Contents

Introducing Symantec AntiVirus for Linux

This chapter 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 through manual and scheduled scans. You can schedule periodic definitions file updates by using the `sav` command-line interface or by using the LiveUpdate Administration Utility and having your client computers retrieve the updates from a local server.

Note: Scanning for security risks is not enabled by default in Symantec AntiVirus for Linux, but may be enabled by using the `GRC.DAT` file. If enabled, security risks can be detected and logged, but Symantec AntiVirus cannot take any actions on them.

Symantec AntiVirus supports Linux client distribution with the RPM Package Manager tools and configuration updates with `GRC.DAT` files.

On Linux distributions, Auto-Protect protects the files that are located on the following types of media:

- Hard drives
- Removable media, such as DVD drives
- Network file servers

All events that are generated are logged to the standard system log through syslog.

See "About the settings in the GRC.DAT file" on page 74.

About this document

To use this guide effectively, you should already understand the following information:

- The basics of how to administer Linux computers, including tasks such as setting your PATH and environment variables.
- How to use the RPM Package Manager application.
- How to download and install the Java Runtime Environment (JRE) on your computers, if it is not already installed.
- If you want to use the client user interface, how to download and install X11, as well as a KDE or Gnome desktop environment, if this software is not already installed.

See "System requirements for Symantec AntiVirus for Linux" on page 9.

Installing Symantec AntiVirus for Linux

This chapter includes the following topics:

System requirements for Symantec AntiVirus for Linux

Symantec AntiVirus requires specific kernels, software, and hardware to run on the Linux operating system. All requirements for Symantec AntiVirus components are designed to work with the hardware and the software recommendations for the supported computers. All Linux computers on which you install Symantec AntiVirus should meet or exceed the recommended system requirements for the operating system.

Table 2-1 System requirements for Symantec AntiVirus for Linux client computers

Component	Requirements
Hardware	■ Intel Pentium II 266 MHz or higher processor ■ 512 MB RAM or higher ■ 3 GB free disk space
Software and distributions	■ Symantec AntiVirus for Linux runs on multiple supported distributions. These distributions are supported on computers using Intel 486-, 586-, and 686-compatible CPUs. See "Supported distributions and kernel versions" on page 10. ■ The Java Runtime Environment (JRE) 1.4 or later must be installed on your Linux computers to use the user interface. The JRE is also required to run Java LiveUpdate. See "About Java LiveUpdate" on page 59. ■ X11 with a KDE or Gnome desktop environment is required to see the system tray icon, user status window, and event notifications. Auto-Protect functionality is available only on supported kernels. See "Unsupported kernel versions" on page 14.

See "Client installation packages for Symantec AntiVirus for Linux" on page 16.

See "Installation package folders for Symantec AntiVirus for Linux" on page 17.

Supported distributions and kernel versions

The material in this section is up to date as of MR14, September 2012. For future information, see the *System requirements for Symantec AntiVirus for Linux 1.0*, at the following URL:

http://www.symantec.com/docs/TECH101598

and the *Release notes for Symantec AntiVirus for Linux 1.0x* at the following URL:

http://www.symantec.com/docs/TECH103599

Symantec AntiVirus for Linux 1.0.14 supports the following distributions:

- Red Hat Enterprise Linux 5.7, kernel 2.6.18-274.18.1.el5
- Red Hat Enterprise Linux 5.8, kernel 2.6.18-308.4.1.el5
- Red Hat Enterprise Linux 6.2, kernel 2.6.32-220.13.1.el6
- Red Hat Enterprise Linux 6.3, kernel 2.6.32-279.el6
- Novell Open Enterprise Server/Linux 2 (OES2), kernel 2.6.16.60-0.83.2

- Novell Open Enterprise Server/Linux 11 (OES11), kernel 2.6.32.59-0.3.1
- Novell Open Enterprise Server/Linux 11 SP1 (OES11SP1), kernel 3.0.26-0.7
- SuSE Linux Enterprise 10 with Service Pack 3, kernel 2.6.16.60-0.83.2
- SuSE Linux Enterprise 10 with Service Pack 4, kernel 2.6.16.60-0.93.1
- SuSE Linux Enterprise 11 with Service Pack 1, kernel 2.6.32.59-0.3.1
- SuSE Linux Enterprise 11 with Service Pack 2, kernel 3.0.26-0.7 [Note: SuSE Linux Enterprise 10/11 includes both Server (SLES10/11) and Desktop (SLED10/11) versions.]
- Ubuntu 11.10, kernel 3.0.0-19-generic, 3.0.0-19-server
- Ubuntu 12.04, kernel 3.2.0-24-generic
- Debian 60r5, kernel 2.6.32-5
- Fedora 16, kernel 3.4.2-1.fc16
- Fedora 17, kernel 3.4.4-3.fc17
- Oracle Linux Server 5.8 2.6.32-300.27.1.el5uek, 2.6.18-308.4.1.0.1.el5
- Oracle Linux Server 6.2 2.6.39-200.24.1.el6uek

Specifically, the following kernel versions are supported (on i386/i686 architecture only):

- Red Hat Enterprise Linux 5.7 default 2.6.18-274.18.1.el5
- Red Hat Enterprise Linux 5.7 PAE 2.6.18-274.18.1.el5PAE
- Red Hat Enterprise Linux 5.7 Xen 2.6.18-274.18.1.el5xen
- Red Hat Enterprise Linux 5.8 default 2.6.18-308.4.1.el5
- Red Hat Enterprise Linux 5.8 PAE 2.6.18-308.4.1.el5PAE
- Red Hat Enterprise Linux 5.8 Xen 2.6.18-308.4.1.el5xen
- Red Hat Enterprise Linux 6.2 default 2.6.32-220.13.1.el6
- Red Hat Enterprise Linux 6.3 default 2.6.32-279.el6
- SuSE Linux Enterprise 10.3 default 2.6.16.60-0.83.2-default
- SuSE Linux Enterprise 10.3 smp 2.6.16.60-0.83.2-smp
- SuSE Linux Enterprise 10.3 bigsmp 2.6.16.60-0.83.2-bigsmp
- SuSE Linux Enterprise 10.4 default 2.6.16.60-0.93.1-default
- SuSE Linux Enterprise 10.4 smp 2.6.16.60-0.93.1-smp
- SuSE Linux Enterprise 10.4 bigsmp 2.6.16.60-0.93.1-bigsmp

- SuSE Linux Desktop 10.3 default 2.6.16.60-0.83.2-default
- SuSE Linux Desktop 10.3 smp 2.6.16.60-0.83.2-smp
- SuSE Linux Desktop 10.3 bigsmp 2.6.16.60-0.83.2-bigsmp
- SuSE Linux Desktop 10.4 default 2.6.16.60-0.93.1-default
- SuSE Linux Desktop 10.4 smp 2.6.16.60-0.93.1-smp
- SuSE Linux Desktop 10.4 bigsmp 2.6.16.60-0.93.1-bigsmp
- SuSE Linux Enterprise 11.1 default 2.6.32.59-0.3.1-default
- SuSE Linux Enterprise 11.1 pae 2.6.32.59-0.3.1-pae
- SuSE Linux Enterprise 11.1 xen 2.6.32.59-0.3.1-xen
- SuSE Linux Enterprise 11.2 default 3.0.26-0.7-default
- SuSE Linux Enterprise 11.2 pae 3.0.26-0.7-pae
- SuSE Linux Enterprise 11.2 xen 3.0.26-0.7-xen
- SuSE Linux Desktop 11.1 default 2.6.32.59-0.3.1-default
- SuSE Linux Desktop 11.1 pae 2.6.32.59-0.3.1-pae
- SuSE Linux Desktop 11.1 xen 2.6.32.59-0.3.1-xen
- SuSE Linux Desktop 11.2 default 3.0.26-0.7-default
- SuSE Linux Desktop 11.2 pae 3.0.26-0.7-pae
- SuSE Linux Desktop 11.2 xen 3.0.26-0.7-xen
- Open Enterprise Server 2 sp2 default 2.6.16.60-0.83.2-default
- Open Enterprise Server 2 sp2 smp 2.6.16.60-0.83.2-smp
- Open Enterprise Server 2 sp2 bigsmp 2.6.16.60-0.83.2-bigsmp
- Open Enterprise Server 2 sp3 default 2.6.16.60-0.83.2-default
- Open Enterprise Server 2 sp3 smp 2.6.16.60-0.83.2-smp
- Open Enterprise Server 2 sp3 bigsmp 2.6.16.60-0.83.2-bigsmp
- Debian 60r5 default 2.6.32-5-686
- Debian 60r5 bigmem 2.6.32-5-686-bigmem
- Fedora 16 default 3.4.2-1.fc16.i686
- Fedora 16 PAE 3.4.2-1.fc16.i686.PAE
- Fedora 17 default 3.4.4-3.fc17.i686
- Fedora 17 PAE 3.4.4-3.fc17.i686.PAE

Additionally, the following kernel versions are supported on x86-64 (both EM64T/AMD64) architectures:

- Red Hat Enterprise Linux 5.7 default 2.6.18-274.18.1.el5
- Red Hat Enterprise Linux 5.7 Xen 2.6.18-274.18.1.el5xen
- Red Hat Enterprise Linux 5.8 default 2.6.18-308.4.1.el5
- Red Hat Enterprise Linux 5.8 Xen 2.6.18-308.4.1.el5xen
- Red Hat Enterprise Linux 6.2 default 2.6.32-220.13.1.el6
- Red Hat Enterprise Linux 6.3 default 2.6.32-279.el6
- SuSE Linux Enterprise 10.3 default 2.6.16.60-0.83.2-default
- SuSE Linux Enterprise 10.3 smp 2.6.16.60-0.83.2-smp
- SuSE Linux Enterprise 10.4 default 2.6.16.60-0.93.1-default
- SuSE Linux Enterprise 10.4 smp 2.6.16.60-0.93.1-smp
- SuSE Linux Desktop 10.3 default 2.6.16.60-0.83.2-default
- SuSE Linux Desktop 10.3 smp 2.6.16.60-0.83.2-smp
- SuSE Linux Desktop 10.4 default 2.6.16.60-0.93.1-default
- SuSE Linux Desktop 10.4 smp 2.6.16.60-0.93.1-smp
- SuSE Linux Enterprise 11.1 default 2.6.32.46-0.3.1-default
- SuSE Linux Enterprise 11.1 xen 2.6.32.46-0.3.1-xen
- SuSE Linux Enterprise 11.2 default 3.0.13-0.27-default
- SuSE Linux Enterprise 11.2 xen 3.0.13-0.27-xen
- SuSE Linux Desktop 11.1 default 2.6.32.59-0.3.1-default
- SuSE Linux Desktop 11.1 xen 2.6.32.59-0.3.1-xen
- SuSE Linux Desktop 11.2 default 3.0.26-0.7-default
- SuSE Linux Desktop 11.2 xen 3.0.26-0.7-xen
- Open Enterprise Server 2 sp2 smp 2.6.16.60-0.83.2-smp
- Open Enterprise Server 2 sp3 default 2.6.16.60-0.83.2-default
- Open Enterprise Server 2 sp3 smp 2.6.16.60-0.83.2-smp
- Open Enterprise Server 11 default 2.6.32.59-0.3.1-default
- Open Enterprise Server 11 xen 2.6.32.59-0.3.1-xen
- Open Enterprise Server 11 sp1 default 3.0.26-0.7-default

- Open Enterprise Server 11 sP1 xen 3.0.26-0.7-xen
- Debian 60r5 default 2.6.32-5-amd64
- Fedora 16 default 3.4.2-1.fc16
- Fedora 17 default 3.4.4-3.fc17
- Ubuntu 11.10 generic 3.0.0-19
- Ubuntu 11.10 server 3.0.0-19
- Ubuntu 12.04 generic 3.2.0-24
- Ubuntu 12.04 generic 3.2.0-24
- Oracle Linux Server release 5.8 u.K. 2.6.32-300.27.1
- Oracle Linux Server release 5.8 el5 2.6.18-308.4.1.0.1
- Oracle Linux Server release 6.2 uek 2.6.39-200.24.1

Running Symantec AntiVirus for Linux 1.0.14 on any other combination of distributions and kernel versions is not supported.

See "Unsupported kernel versions" on page 14.

See "Client installation packages for Symantec AntiVirus for Linux" on page 16.

Unsupported kernel versions

All the kernels that are listed in the SAVFL MR14 Legacy Kernels page of the `Kernel_Checklist_MR14.xls` file are no longer supported for maintenance in 1.0.14. This file appears as a table that is located at the following URL:

http://www.symantec.com/docs/TECH101598

If you want to real-time protection for one of these kernels, use the legacy `rpm` packages or the `deb` packages that can be found in the `\unsupported` folder.

See "Supported distributions and kernel versions" on page 10.

Installation scenarios for installation client packages

Based on your company's environment and needs, you may not want to install all Symantec AntiVirus for Linux packages. This section describes some typical installation scenarios.

Table 2-2 Supported distributions with supported and unsupported kernels

Distribution type	Supported and unsupported feature
Supported distribution and a supported kernel version	You can install all files and use all the features, which include manual and scheduled scanning, Auto-Protect, the X11-based graphical user interface, and Java LiveUpdate. Your Linux computers must use supported Linux distributions and supported kernel versions, and have X11 and JRE 1.4 or later installed. The files can be installed in any order, as long as the sav package is installed before the savui package. If you install all files at once, the files are automatically installed in the appropriate order.
Supported distribution, but an unsupported kernel version	In this scenario, the Auto-Protect functionality is not available. You can still use the Symantec AntiVirus manual and scheduled scanning capabilities and Java LiveUpdate to protect the computer. If you use an unsupported kernel version, Auto-Protect does not function. However, if you install the savap package on a computer and then later load a supported kernel, Auto-Protect does function. You should install the following packages: ■ sav ■ savap
Supported distribution and a supported kernel version, but do not use Java	In this scenario, you cannot use Java LiveUpdate to update definitions. You must use an alternative method. You should install the following packages: ■ sav ■ savap
Supported distribution and a supported kernel version, but do not use X11	In this scenario, the Symantec AntiVirus user interface is not available on your Linux computers. You can use the sav command line tool to update definitions. You can use sav command line tool and the computer's syslog to access status and alert messages. You should install the following packages: ■ sav ■ savap
Supported distribution, but have a minimum amount of computing resources	In this scenario, you run a supported distribution and want a minimal footprint that provides only manual and scheduled scanning. You can do this whether you are running a supported or an unsupported version of the kernel. You must use the sav command line tool and the computer's syslog to access status and alert messages, and to update definitions without using Java LiveUpdate. You should install only the base sav package.

See “Supported distributions and kernel versions” on page 10.

See “Unsupported kernel versions” on page 14.

See “Installation package folders for Symantec AntiVirus for Linux” on page 17.

See “About Java LiveUpdate” on page 59.

Client installation packages for Symantec AntiVirus for Linux

Symantec AntiVirus uses the rpm Package Manager format for installation. Symantec AntiVirus consists of several installation files, which use the following name format:

<package name>-<major version>.<minor version>.<crt release>-<build number>.<architecture>.rpm

For example, a typical file name might be sav-1.0.0-94.i386.rpm.

Table 2-3 Symantec AntiVirus for Linux client installation packages

Package	Dependencies	Description
sav (mandatory)	None	The main Symantec AntiVirus program, which implements scanning capabilities.
savap (optional)	kernel version	Symantec AntiVirus Auto-Protect features. Only specific kernel versions are supported. **Note:** If you use an unsupported kernel version, Auto-Protect does not function. However, if you install the savap package on a computer and then later load a supported kernel, Auto-Protect does function. See “Supported distributions and kernel versions” on page 10.
savui (optional)	sav X11 JRE 1.4 or later	The Symantec AntiVirus graphical user interface. X11 must already be installed.
savjlu (optional)	sav JRE 1.4 or later	The Java LiveUpdate features. If this package is not installed, alternative methods must be used to update definitions. See “About updating virus definitions on Linux” on page 57. See “About Java LiveUpdate” on page 59.

See “Installation package folders for Symantec AntiVirus for Linux” on page 17.

Installation package folders for Symantec AntiVirus for Linux

Table 2-4 lists the different installation package folders for Symantec AntiVirus for Linux.

Table 2-4 Client installation package folders

Package folder	Package contents and notes
`/deb/`	`/deb/` contains the deb packages for both Debian distributions and Ubuntu distributions. Make sure that the user is in the `sudo-ers` list. For Debian or Ubuntu 32bit architectures, execute **`'sudo dpkg -i sav-*.i386.deb savap-*.i386.deb savjlu-*.i386.deb savui-*.i386.deb.`** For Debian or Ubuntu 64bit architectures, execute **`sudo dpkg -i sav-*.amd64.deb savap-*.amd64.deb savjlu-*.amd64.deb savui-*.amd64.deb`**.
`/rpm/`	`/rpm/` contains the rpm packages for most of the Linux distributions that support the Red Hat Package Manager. For i386/i686 32bit architectures, execute **`rpm -I sav-*.i386.rpm savap-*.i386.rpm savjlu-*.i386.rpm savui-*.i386.rpm`**. For x86-64 EM64T/AMD64 architectures, execute'**`rpm -I sav-*.i386.rpm savap-x64-*.x86_64.rpm savjlu-*.i386.rpm savui-*.i386.rpm`**.
`/unsupported/`	`/unsupported/` contains the legacy rpm and deb packages that new fixes no longer support, starting with 1.0.14. For the legacy kernels on i386/i686 32bit architectures, type the following command: **`rpm -I ../rpm/sav-*.i386.rpm savap-legacy-*.i386.rpm ../rpm/savjlu-*.i386.rpm ../rpm/savui-*.i386.rpm`**. For the legacy kernels on x86-64 EM64T/AMD64 architectures, type the following command: **`rpm -I ../rpm/sav-*.i386.rpm savap-x64-legacy-*.x86_64.rpm ../rpm/savjlu-*.i386.rpm ../rpm/savui-*.i386.rpm`**. For the legacy kernels on i386/i686 32bit architectures for Debian or Ubuntu, type the following command: **`sudo dpkg -i ../deb/sav-*.i386.deb savap-legacy-*.i386.deb ../deb/savjlu-*.i386.deb ../deb/savui-*.i386.deb`**. For the legacy kernels on x86-64 EM64T/AMD64 architectures for Debian, type the following command: **`sudo dpkg -i ../deb/sav-*.amd64.deb savap-x64-legacy-*.amd64.deb ../deb/savjlu-*.amd64.deb ../deb/savui-*.amd64.deb`**.

You can use a customized installation path for rpm packages only. To customize the path, ensure that all rpm packages use the same path, as follows: **`rpm -I --prefix <custom path> sav*.rpm`**. If the installation displays the message "Relocation not supported for this configuration, please use --prefix

<foldername>," then the <foldername> should be used as the --prefix value, as this indicates that there are other Symantec applications on the machine using that value. Alternatively, if there are no other Symantec products on the machine, modify the `BaseDir` value to the desired custom path, and then rerun the installation.

See "Supported distributions and kernel versions" on page 10.

See "Unsupported kernel versions" on page 14.

See "Client installation packages for Symantec AntiVirus for Linux" on page 16.

Installing Symantec AntiVirus for Linux locally

The installation of Symantec AntiVirus for Linux is silent. You can use the rpm command-line parameter, `-Uhv`, to display the current percentage of the installation that is complete. You do not need to restart the Linux client after installation.

The **`rpm -U`** command-line argument can be used to perform an initial installation or to update an existing installation of Symantec AntiVirus for Linux. Although you can also use the **`rpm -I`** command to install, Symantec recommends that you use `-U`. The `-I` command results in an error if a previous version of Symantec AntiVirus for Linux is already present.

You can install the packages separately or all at once, using wildcard characters, and they install in the correct order.

To install each file separately

◆ On the command line, type the following command:

```
rpm –Uhv <file_name>.rpm
```

See "System requirements for Symantec AntiVirus for Linux" on page 9.

See "Installing Symantec AntiVirus for Linux from a remote server" on page 18.

Installing Symantec AntiVirus for Linux from a remote server

With rpm, you can install packages for the first time from a remote FTP or HTTP server. To do this, you need to supply the name of the remote server on the command line. You can install from an HTTP server by replacing FTP in the following examples with HTTP, and replacing the <someserver.com> with an HTTP server instead of an FTP server.

To install Symantec AntiVirus for Linux from a remote server

- On the command line, type the following command:

  ```
  rpm -I ftp://<someserver.com/someshare/file name>.rpm
  ```

  If you need to use login credentials for the remote server, type the following command:

  ```
  rpm -I ftp://<user name:password@someserver.com/someshare/file
  name>.rpm
  ```

See "System requirements for Symantec AntiVirus for Linux" on page 9.

See "Installing Symantec AntiVirus for Linux locally" on page 18.

See "Uninstalling Symantec AntiVirus for Linux" on page 20.

Repackaging the Symantec AntiVirus for Linux client installation package

The `repackage.sh` script file is provided so that you do not have to manually edit the configuration file. This script repackages the client installation package to contain your custom configurations for distribution to clients.

To repackage the Symantec AntiVirus for Linux client installation package

1. Install the related utilities for repacking:
   - GNU core utilities
   - VI (or VIM) editor
   - `sed`
   - `grep`
   - `which`
   - `cpio` (only needed for rpm package)
   - `rpm2cpio` (only needed for rpm package)
   - `rpmbuild` (only needed for rpm package)
   - `dpkg-deb` (only needed for DEB package)
2. Run the `repackage.sh` script:

   ```
   # ./repackage.sh packagefile
   ```

Uninstalling Symantec AntiVirus for Linux

Uninstalling Symantec AntiVirus removes installed files from the computer and unregisters the package from the rpm database. If you try to uninstall a package that is not currently installed, Symantec AntiVirus displays a message that a package is not installed. However, the uninstallation of the other packages still succeeds.

To uninstall Symantec AntiVirus for Linux

1. If you have all packages installed, on the command line, type the following:

   ```
   rpm -e sav savap savui savjlu
   ```

2. Restart the computer to remove the Auto-Protect support.

See "About removing Symantec AntiVirus completely" on page 20.

Listing all Symantec AntiVirus packages

If you don't remember the package names or which packages are installed, you can use the `rpm -qa` command to list the installed Symantec AntiVirus packages.

To list all Symantec AntiVirus packages

- On the command line, type the following command:

  rpm –qa | grep sav

About removing Symantec AntiVirus completely

After using the `rpm -e` command to uninstall Symantec AntiVirus, some directories and files still remain. If you need to completely remove Symantec AntiVirus from a computer, you can delete the following directories:

`/var/symantec`	alert logs and quarantined files
`/opt/Symantec/symantec_antivirus`	technical support log files
`/etc/symantec`	the configuration database

You can also safely delete any empty directories that are located under `/opt/Symantec`.

The following directories may also remain. You should only delete the directories if you are sure that there is no Symantec product on the computer that currently uses LiveUpdate:

- `/opt/Symantec/virusdefs`

- /opt/Symantec/LiveUpdate

The /etc/symantec.conf file may remain. You should only delete the file if you are sure that there are no other Symantec products installed on the computer.

Chapter 3

Using Symantec AntiVirus for Linux

This chapter includes the following topics:

When to use the command-line interfaces, services, and tools

Symantec AntiVirus provides several command-line interfaces (CLIs), services, and tools for configuring and interacting with Symantec AntiVirus when running on Linux.

Note: You must have root privileges to use most of the Symantec AntiVirus for Linux service and command-line interface commands. The exceptions are the `sav liveupdate -u` and `info -a`,`-d`,`-e`, `-p`, and `-s` commands.

Table 3-1 Symantec AntiVirus interfaces, services, and tools

Interface or tool	Function
sav command-line interface	This interface provides the primary method of interacting with the Symantec AntiVirus service. You should use this interface for the following tasks: ■ Enabling and disabling Auto-Protect ■ Starting and scheduling LiveUpdates and viewing the current LiveUpdate schedule ■ Starting and stopping manual scans ■ Creating, deleting, enabling, and disabling scheduled scans ■ Viewing a list of scheduled scans and detailed information about each scan ■ Displaying items and acting on items in the local Quarantine ■ Rolling back to a previous version of virus and security risk definitions ■ Using the latest version of local of virus and security risk definitions ■ Displaying general product information
symcfg command-line interface	This interface provides client applications with access to a computer-specific, local configuration database that is used to store configuration data for Symantec AntiVirus for Linux. **Note:** You should use this interface when you need to access Symantec AntiVirus configuration settings that are not accessible through the sav CLI. You should use this interface for the following tasks: ■ Displaying data in the configuration database ■ Adding data to the configuration database ■ Removing data from the configuration database
symcfgd service	This service typically runs as a daemon process. This daemon is not typically run from the command line. It is started automatically by the system initialization scripts. If necessary, you can use the parameters that are associated with this service for the following tasks: ■ Specifying the log facility to use when logging to syslog ■ Filtering events that are logged based on severity ■ Stopping the symcfgd daemon ■ Checking to see if the symcfgd service is currently running ■ Changing the working directory for symcfgd ■ Changing the file that holds the PID of the currently running copy of symcfgd

Table 3-1 Symantec AntiVirus interfaces, services, and tools *(continued)*

Interface or tool	Function
rtvscand service	This service is the interface to rtvscan, the Symantec AntiVirus service that protects Linux client computers from viruses and other security risks. This daemon is not typically run from the command line. It is started automatically by the system initialization scripts. If necessary, you can use the parameters that are associated with this service for the following tasks: ■ Specifying the log facility to use when logging to syslog ■ Filtering the events that are logged based on severity ■ Stopping the rtvscand daemon ■ Displaying help information ■ Checking to see if the rtvscand service is currently running ■ Changing the working directory for rtvscand ■ Changing the file that holds the PID of the currently running copy of rtvscand
savtray command-line interface	This interface runs the Symantec AntiVirus graphical user interface for Symantec AntiVirus for Linux client computers. You should use this interface for the following tasks: ■ Launching the graphical interface with parameters for session management ■ Launching the graphical interface with parameters for controlling the appearance and graphical behavior of Symantec AntiVirus

About the sav command-line interface

Symantec AntiVirus for Linux provides a command-line interface for interacting with sav, the basic Symantec AntiVirus service. You can use the sav command-line interface to perform the following tasks:

- enable and disable Auto-Protect, use LiveUpdate
- start and stop manual scans
- list information about scheduled scans
- create and delete scheduled scans
- enable and disable scheduled scans
- manage the local Quarantine
- manage virus definitions
- display product information

The sav commands that produce output produce it in a format that can be parsed by third-party tools. There is no header information for the columns in this output.

About the sav command-line syntax

The general syntax for the sav command line is as follows:

```
sav [--quiet] command parameter(s)
```

The `--quiet` parameter is the only global parameter for the sav command line.

sav itself does not take wildcard characters, so any wildcard characters that are used on the sav command line are interpreted by the shell that you are using.

You can perform only one action per command line invocation. For example, you cannot turn on Auto-Protect and initiate a LiveUpdate on the same command line.

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

Note: You must have root privileges to use all of the sav CLI commands except `sav liveupdate -u` and `sav info -a,-d,-e, -p, and -s`.

Table 3-2 sav commands and parameters

Command	Parameters	Description
`sav`	`-q|--quiet`	Display only the information that is requested; do not display all available information, including status and error messages. This is the only global parameter. This parameter is particularly useful in scripts where you do not want textual error or status messages to appear when the script runs.
`sav autoprotect`	`-e|--enable`	Enable Auto-Protect.
`sav autoprotect`	`-d|--disable`	Disable Auto-Protect.
`sav liveupdate`	`-u|--update`	Perform a LiveUpdate immediately.
`sav liveupdate`	`-v| --view`	Display the current LiveUpdate schedule.

Table 3-2 sav commands and parameters *(continued)*

Command	Parameters	Description
`sav liveupdate`	`-s|--schedule <parameters>`	Create a new schedule for an automatic LiveUpdate. The following parameters are used to set the schedule: ■ `-f <daily|weekly|monthly>|--frequency <daily|weekly|monthly>` Mandatory. Specifies the frequency. ■ `-i <HH[:]MM|DDD|D>|--interval <HH[:]MM|DDD|D>` Mandatory. Identifies the interval of the schedule. If frequency is daily, the interval must be hh[:]mm, where hh is the hour (00-23) and mm is the minute. If frequency is weekly, DDD must be one of the following: Sun, Mon, Tue, Wed, Thu, Fri, Sat. If frequency is monthly, D is any value between 1 and 31. ■ `-t hh[:]mm|--time hh[:]mm` where hh is the hour (00-23) and mm is the minute (00-59). If no time is specified, this parameter defaults to midnight of the designated interval. Not used for daily frequency.

Table 3-2 sav commands and parameters *(continued)*

Command	Parameters	Description
`sav manualscan`	`-s|--scan [<path_name>…|-]`	Initiate a manual scan of the current directory and all its subdirectories. To specify a file and directory list to be scanned, type a list of files and directories, following each item with Enter and ending the list with CTRL-D. If a directory is specified, all subdirectories of that directory are also scanned. Wildcard characters that are used in file names are expanded by the shell. If you use a hyphen instead of a <path_name> argument, then the list of path names is read from the standard input. This is useful when you want to use the output of some other Linux command that produces a list of file names as input to the sav command. You must use commands that produce a list of files or path names separated by line feeds. By default, the maximum number of items that can be added to a manual scan that is generated from the command line interface is 100. You can use symcfg to change the DWORD value `\Symantec Endpoint Protection\AV\MaxInput` to increase this limit. To remove the limit entirely, you must set it to 0. See "Using the symcfg CLI to interact with the Symantec AntiVirus configuration database" on page 43. **Note:** Submitting a very long list of items to the manualscan command can negatively impact system performance, so Symantec recommends that you limit lists to a maximum of a few thousand items.
`sav manualscan`	`-c|--clscan [pathname|-]`	Initiates a synchronous manual scan that does not return control to the command prompt until the scan is complete.
`sav manualscan`	`-t|--stop`	Stop a manual scan that is in progress.
`sav scheduledscan`	`-e|--enable <scan ID>`	Enable a specific scheduled scan.
`sav scheduledscan`	`-s|--disable <scan ID>`	Disables a specific scheduled scan.
`sav scheduledscan`	`-p|--stop scan_id`	Stops a scheduled scan that is in progress.
`sav scheduledscan`	`-l|--list`	List all scheduled scans and their current status, either enabled or disabled.
`sav scheduledscan`	`-n|--info <scan ID>`	Display detailed information about a specific scan.

Table 3-2 sav commands and parameters *(continued)*

Command	Parameters	Description
`sav scheduledscan`	`-d|--delete <scan ID>`	Delete a specific scheduled scan.

Table 3-2 sav commands and parameters *(continued)*

Command	Parameters	Description
`sav scheduledscan`	`-c|--create <scan ID> <parameters> [<path_name>...|-]`	

Table 3-2 sav commands and parameters *(continued)*

Command	Parameters	Description
		Create a new scan identified by the id, which must be unique. The following parameters are available: ■ `-f <daily|weekly|monthly> |--frequency <daily|weekly|monthly>` Specifies the frequency. ■ `-i <HH[:]MM|DDD|D> |--interval <HH[:]MM|DDD|D>` Identifies the interval of the schedule. If frequency is daily, the interval must be hh[:]mm, where hh is the hour (00-23) and mm is the minute. If frequency is weekly, DDD must be one of the following: Sun, Mon, Tue, Wed, Thu, Fri, Sat. If frequency is monthly, D is any value between 1 and 31. ■ `-t hh[:]mm|--time hh[:]mm` Where hh is the hour (00-23) and mm is the minute (00-59). If no time is specified, this parameter defaults to midnight of the designated interval. Not used for daily frequency. ■ `-m|--missedevents` Enables or disables missed event processing. If enabled, then the scan will run at a later time if the computer is not on at the scheduled time. 0: disabled and 1: enabled. The default value is 0. To specify a list to be scanned, type a list of files and directories, following each item with Enter and ending the list with CTRL-D. If a directory is specified, all subdirectories of that directory are also scanned. Wildcard characters that are used in file names are expanded by the shell. If you use a hyphen instead of a <path_name> argument, then the list of path names is read from the standard input. This is useful when you want to use the output of some other Linux command that produces a list of file names as input to the sav command. You must use commands that produce a list of files or path names separated by line feeds. By default, the maximum number of items that can be added to a scheduled scan that is generated from the command line interface is 100. You can use symcfg to change the DWORD value VirusProtect6\MaxInput to

Table 3-2 sav commands and parameters *(continued)*

Command	Parameters	Description
		increase this limit. To remove the limit entirely, you must set it to 0. **Note:** Submitting a very long list of items to the scheduledscan command can negatively impact system performance, so Symantec recommends that you limit lists to a maximum of a few thousand items.
`sav quarantine`	`-l|--list`	List all items that are in the local Quarantine.
`sav quarantine`	`-d|--delete <ID>`	Delete the specified quarantined item. To get the ID of an item in the Quarantine, list the items that are in the Quarantine.
`sav quarantine`	`-r|--restore <ID>`	Restore the specified quarantined item. To get the ID of an item in the Quarantine, list the items that are in the Quarantine.
`sav quarantine`	`-p|--repair <ID>`	Attempt to repair the specified quarantined item. To get the ID of an item in the Quarantine, list the items that are in the Quarantine.
`sav quarantine`	`-i|--info <ID>`	Provide detailed information about the specified quarantined item. To get the ID of an item in the Quarantine, list the items that are in the Quarantine.
`sav quarantine`	`-d|--delete/-r|--restore/ -p|--repair/-i|--info "*"`	Deletes, restores, repairs, or provides detailed information about all of the quarantined items, respectively.
`sav definitions`	`-r|--rollback`	Roll the definitions file that is used back to the last known good version.
`sav definitions`	`-u|--usenewest`	Signal RTVScan to check for new definitions locally and to use them, if new definitions are available.
`sav info`	`-a|--autoprotect`	Display the status of Auto-Protect on the computer.
`sav info`	`-d|--defs`	Display the version and date of the current virus definitions in use on the computer.
`sav info`	`-e|--engine`	Display the version of the scan engine that is currently on the computer.
`sav info`	`-p|--product`	Display the version of the product that is currently on the computer.

Table 3-2 sav commands and parameters *(continued)*

Command	Parameters	Description
`sav info`	`-s|--scanner`	Display whether or not a scan is in progress on the computer.
`sav info`	`-t|--threats`	Display the list of threats and security risks that the computer is currently protected against. **Note:** A user must have root privileges to use this parameter.

Using the sav CLI to interact with Symantec AntiVirus

You can use the sav CLI to perform the following tasks:

- enable and disable Auto-Protect
- start and schedule LiveUpdates and view the current LiveUpdate schedule
- start and stop manual scans
- create, delete, enable, and disable scheduled scans
- view a list of scheduled scans and detailed information about each scan
- display items and act on items in the local Quarantine
- roll back to a previous version of virus and security risk definitions
- use the latest version of local virus and security risk definitions
- display general product information

Note: You must have root privileges to use all of the sav CLI commands except `liveupdate -u` and `info -a,-d,-e, -p,` and `-s`.

Enabling and disabling Auto-Protect

You can use the `sav autoprotect` command to enable and disable Auto-Protect on a specific computer.

To enable Auto-Protect

- From the command line, type the following:

```
sav autoprotect --enable
```

To disable Auto-Protect

- From the command line, type the following:

  ```
  sav autoprotect --disable
  ```

Using Java LiveUpdate

You can use the sav liveupdate command to initiate an update using Java LiveUpdate on a specific computer, to view the computer's current LiveUpdate schedule, and to schedule automatic updates using Java LiveUpdate.

There is no managed process for distributing new definitions to clients from a central computer. However, you can do the following tasks:

- Use the Intelligent Updater shell script from http://securityresponse.symantec.com/ to update multiple computers.
- Use the LiveUpdate Administration Utility to set up a Central LiveUpdate server on your network and configure Java LiveUpdate to point your clients to pick up definitions updates from that server.

To start an immediate LiveUpdate

- From the command line, type the following:

  ```
  sav liveupdate --update
  ```

To view the current LiveUpdate schedule

- From the command line, type the following:

  ```
  sav liveupdate --view
  ```

To schedule an automatic LiveUpdate

- From the command line, type the following:

  ```
  sav liveupdate --schedule -f <frequency> -i <interval> -t <time>
  ```

  For example, to schedule an automatic LiveUpdate that runs every Friday at 11:30 P.M., type the following:

  ```
  sav liveupdate --schedule -f weekly -i Fri -t 23:30
  ```

  For example, to schedule an automatic LiveUpdate that runs only on the second day of the month at 3 A.M., type the following:

  ```
  sav liveupdate --schedule -f monthly -i 2 -t 3:00
  ```

See "Updating definitions by using Intelligent Updater" on page 68.

See "About the LiveUpdate Administration utility" on page 58.

See "Configuring Java LiveUpdate to use a Central LiveUpdate server" on page 63.

Starting and stopping manual scans

You can use the `sav manualscan` command to start and to stop a manual scan on a specific computer.

If you use a hyphen (-) as the <path_names> argument when starting a manual scan, the list of <path_names> is read from the standard input. This is useful if you want to use the output of another Linux command that produces a list of file names as input to sav. Use commands that produce a list with a line feed between each item.

By default, the maximum number of items that can be added to a manual scan that is generated from the command line interface is 100. You can use symcfg to change the DWORD value \Symantec Endpoint Protection\AV\MaxInput to increase this limit. To remove the limit entirely, you must set it to 0.

See "Using the symcfg CLI to interact with the Symantec AntiVirus configuration database" on page 43.

Note: Submitting a very long list of files to the manualscan command can negatively impact system performance, so Symantec recommends that you limit file lists to a maximum of a few thousand items.

To start a manual scan of a directory and its subdirectories

- From the command line, type the following:

  ```
  sav manualscan --scan <path_name>
  ```

  For example, to start a manual scan of user John's directory in the /home directory, type the following:

  ```
  sav manualscan --scan /home/john
  ```

To start a manual scan with input from another command

- From the command line, type the following:

  ```
  <other command> | sav manualscan --scan -
  ```

  Use commands that produce a list of items separated by line feeds. For example, to start scan of all files that have been modified within the last hour in or below a user's home directory, type the following:

  ```
  find ~john -mmin -60 -type f -print | sav manualscan --scan -
  ```

To type a list of files and directories to be scanned

- From the command line, type the following:

```
sav manualscan --scan -

<file name> ENTER

<path name> ENTER

<path name> ENTER

<filename> CTRL-D
```

To stop a manual scan that is in progress

- From the command line, type the following:

```
sav manualscan --stop
```

Creating and managing scheduled scans

You can create, enable and disable, list, and display detailed information about a particular scheduled scan from the command line.

By default, the maximum number of items that can be added to a scheduled scan that is generated from the command line interface is 100. You can use symcfg to change the DWORD value \Symantec Endpoint Protection\AV\MaxInput to increase this limit. To remove the limit entirely, you must set it to 0.

Note: Submitting a very long list of files to the scheduledscan command when creating a scheduled scan can negatively impact system performance, so Symantec recommends that you limit lists to a maximum of a few thousand items.

Listing information about scheduled scans

Table 3-3 lists the fields that the scheduled scans output.

Table 3-3 Scheduled scan output

Scan ID	Frequency and time of the scan	Scan status	Scan state
SS01	Weekly: Mon	Enabled	Done
SS02	Daily: 11:15	Disabled	Never Run
SS03	Monthly: 25	Disabled	Never Run

To list the scheduled scans on a computer

- From the command line, type the following:

  ```
  sav scheduledscan --list
  ```

To list detailed information about a particular scan

- From the command line, type the following:

  ```
  sav scheduledscan --info <scan ID>
  ```

Creating and deleting a scheduled scan

You can use the `sav scheduledscan` command to create and delete a scheduled scan on a specific computer.

To create a scheduled scan

- From the command line, type the following:

  ```
  sav scheduledscan --create <scan ID> -f <frequency> -i <interval>
  -t <time> -m <missed event processing value> <path name>...
  ```

  For example, suppose you want to create a scheduled scan named myschedscan that scans the /usr directory, runs every Saturday at 11:01 P.M., and will not run when the computer is next turned on, if the computer is not on at the scheduled time. To create this scan, from the command line, type the following:

  ```
  sav scheduledscan --create myschedscan -f weekly -i Sat -t 23:01
  -m 0 /usr
  ```

To create a scheduled scan by using input from another command

- From the command line, type the following:

  ```
  <other command> | sav scheduledscan --create <scan ID> -f
  <frequency> -i <interval> -t <time> -m <missed event processing
  value> -
  ```

  Use commands that produce a list of items separated by line feeds. For example, to schedule a daily scan of all files that have been modified within the last eight hours in or below Steve's home directory, type the following:

  ```
  find ~steve -mmin -480 -type f -print | sav scheduledscan --create
  stevescan -f daily -i 17:01 -m 0 -
  ```

To delete a scheduled scan

◆ From the command line, type the following:

```
sav scheduledscan --delete <scan ID>
```

where `<scan ID>` is the name you gave to the scan when you created it.

Enabling and disabling a scheduled scan

You can use the `sav scheduledscan` command to enable and disable a scheduled scan.

To enable a scheduled scan

◆ From the command line, type the following:

```
sav scheduledscan --enable <scan ID>
```

where `<scan ID>` is the name you gave to the scan when you created it.

To disable a scheduled scan

◆ From the command line, type the following:

```
sav scheduledscan --disable <scan ID>
```

where `<scan ID>` is the name that you gave to the scan when you created it.

Managing the local Quarantine

You can use the `sav quarantine` command to do the following:

- list the items in the Quarantine
- display detailed information about an item in the Quarantine on a specific computer
- delete and restore items from the Quarantine
- attempt to repair an item in the Quarantine

To list the files in the local Quarantine

◆ From the command line, type the following:

```
sav quarantine --list
```

To display detailed information about a file in the local Quarantine

- From the command line, type the following:

  ```
  sav quarantine --info <ID>
  ```

  where `<ID>` is the ID of the item. Obtain the ID of an item by listing the items that are in the local Quarantine.

To delete a file in the local Quarantine

- From the command line, type the following:

  ```
  sav quarantine --delete <ID>
  ```

  where `<ID>` is the ID of the item. Obtain the ID of an item by listing the items that are in the local Quarantine.

To restore a file in the local Quarantine

- From the command line, type the following:

  ```
  sav quarantine --restore <ID>
  ```

  where `<ID>` is the ID of the item. Obtain the ID of an item by listing the items that are in the local Quarantine.

To repair a file in the local Quarantine

- From the command line, type the following:

  ```
  sav quarantine --repair <ID>
  ```

  where `<ID>` is the ID of the item. Obtain the ID of an item by listing the items that are in the local Quarantine.

Managing virus definitions

You can use the `sav definitions` command to roll back the virus and security risk definitions to the last known good version or to have the computer check for and use the latest local version of definitions on a specific computer.

To roll back to the last known good version of definitions

- From the command line, type the following:

  ```
  sav definitions --rollback
  ```

To use the latest local version of definitions

- From the command line, type the following:

  ```
  sav definitions --usenewest
  ```

Displaying product information

You can use the `sav info` command to display general product information about a specific computer, including the following items:

- The status of Auto-Protect
- The version and date of the current virus definitions
- The product version that is in use
- The version of the scan engine that is in use
- Whether or not a scan is in progress
- The list of threats and security risks that the computer is currently protected against

To display the status of Auto-Protect

◆ From the command line, type the following:

```
sav info --autoprotect
```

To display the virus definitions version

◆ From the command line, type the following:

```
sav info --defs
```

To display the current product version

◆ From the command line, type the following:

```
sav info --product
```

To display the current scan engine version

◆ From the command line, type the following:

```
sav info --engine
```

To determine if a scan is in progress

◆ From the command line, type the following:

```
sav info --scanner
```

To display the list of threats that the computer is protected from

◆ From the command line, type the following:

```
sav info --threats
```

About the symcfg command-line interface

symcfg is a command-line tool that provides client applications with access to a computer-specific, local configuration database that is used to store configuration data for Symantec AntiVirus. Configuration settings are stored in a data file in binary format, not as text. The symcfg tool can be used to display, create, remove, and change the value of data that is stored in this database.

About the symcfg command-line syntax

You cannot use multiple `symcfg` commands and their parameters as part of the same command line.

You must use the following syntax for the `symcfg` command lines:

```
symcfg [-q|--quiet] [-r|--recursive]

symcfg [-q|--quiet] [-r|--recursive] add -k|--key key [-v|--value
value -d|--data data -t|--type type]

symcfg [-q|--quiet] [-r|--recursive] delete -k|--key key [-v|--value
value]

symcfg [-q|--quiet] [-r|--recursive] list -k|--key [key|*] [-v|--value
value]
```

Note: You must have root privileges to use symcfg.

By default, **symcfg** is located in `/opt/Symantec/symantec_antivirus`.

Note: You may need to enclose key names in single quotes to prevent the backslash from being interpreted as an escape character by the shell.

Table 3-4 symcfg commands and parameters

Command	Parameters	Description
symcfg	-q [command] --quiet [command]	Display only the information that is being requested; suppress error messages.
symcfg	-r --recursive	Apply the command that follows recursively.

Table 3-4 symcfg commands and parameters *(continued)*

Command	Parameters	Description
`symcfg add`	N/A	Create new keys and values in the database, or overwrite existing ones.

`symcfg add`
Mandatory.
	`-k key`
	`--key key`
		The name of the key to add or overwrite.
		Note: If no corresponding value is given, only the key is created.

`symcfg add`	`-v value`
	`--value value`
		The name of the value to add or overwrite.

`symcfg add`	`-d data`
	`--data data`
		The data to store for the value/data pair.

`symcfg add`	`-t type`
	`--type type`
		One of the following constants, representing the data type the following:
		■ `reg_sz (string)`
		■ `reg_dword (`32-bit unsigned integer)
		■ `reg_binary` (arbitrary binary data)

`symcfg delete`	N/A	Remove keys and values from the database.

`symcfg delete`	`-k key`
	`--key key`
		The name of the key to delete. Mandatory.
		Note: If no corresponding value is given, the key and all of its values are deleted. If there are subkeys present, the delete fails.

`symcfg delete`	`-v value`
	`--value value`
		The name of the value to remove.

`symcfg list`	N/A	List all the values and keys for a given key.

`symcfg list`	`-k key`
	`--key [key|*]`
		The name of the key to list. To list all keys from the root node, use an asterisk (*) instead of a key name. Mandatory.
		If used without the --value parameter, all subkeys and values for this key are listed.
		Note: You must escape an asterisk or enclose it in quotes to protect it from being expanded by the shell.

Table 3-4 symcfg commands and parameters *(continued)*

Command	Parameters	Description

`symcfg list`	`-v value`
	`--value value`
		The name of the value to list. The value is displayed in the following format : `\<key>\<subkey>\<value name> <value data> <value type>`.
		For example:
		`\Symantec Endpoint Protection\AV\Storages\FileSystem\ServiceStatus 1 REG_DWORD`

Using the symcfg CLI to interact with the Symantec AntiVirus configuration database

The symcfg CLI provides access to some configuration settings that are stored in the local configuration database that are not accessible through the sav CLI.

Note: You must have root privileges to use the symcfg command-line interface.

Listing the keys in the database

You can list all of the keys that are stored in the database.

To list the keys in the database

- From the command line, type the following:

  ```
  symcfg list -k <key> [-v <value>]
  ```

  For example, to list all keys under the Storages node, you would type the following:

  ```
  symcfg -r list -k '\Symantec Endpoint Protection\AV\Storages'
  ```

Adding a key to the database

You can add keys and their corresponding values to the database to configure Symantec AntiVirus.

To add a key to the database

◆ From the command line, type the following:

```
symcfg add -k <key> [-v <value>] [-d <data>] [-t <type>]
```

For example, to add a key to the database to exclude the `/tmp/no_scan` directory from Auto-Protect scans, you would type the following:

```
symcfg add --key
VirusProtect6\Storages\Filesystem\RealTimeScan\NoScanDir --value
/tmp/no_scan --data 1 --type REG_DWORD
```

Deleting a key from the database

You can delete keys and their corresponding values from the database to configure Symantec AntiVirus.

To delete a key from the database

◆ From the command line, type the following:

```
symcfg delete -k <key> [-v <value>] [-d <data>] [-t <type>]
```

For example, to delete the scan1 from the database, you would type the following:

```
symcfg delete -k "VirusProtect6\Custom Tasks\scan1"
```

About the symcfgd service

symcfgd is the Symantec configuration service, which runs as a daemon process. This service is typically started automatically by the system initialization scripts. No changes to the default values should be required.

Note: This implementation uses a small number of kernel semaphores, which are shared among applications. Although unlikely, it is possible that Auto-Protect could experience problems if the operating system has an insufficient number of semaphores allocated for the computer. If the allocation of a semaphore fails, an event appears in the syslog. If necessary, you can increase the number of semaphores that are allocated for the operating system to alleviate the problem.

symcfgd service configuration parameters

The parameters available for interacting with the symcfgd are used by the `/etc/sysconfig/symcfgd` file, but can also be used from the command line if special handling is required.

Table 3-5 symcfgd service configuration parameters

Parameter	Description
`-f <log_facility>`	Specifies the log facility to use when logging to syslog. Possible values are as follows: ■ daemon (default) ■ user ■ local0 through local7 To set this up, you must also configure your `/etc/syslog.conf` file to specify handling for the facility.
`-h`	Displays help information.
`-k shutdown | check`	Sends a specified signal to the running copy of symcfgd, and then exits. The running copy is identified as the process that has the pid that matches the pid stored in the pid file. This parameter has the following arguments: ■ Shutdown sends a signal to shut down the running copy. The process attempts to perform a graceful shutdown. ■ Check determines if symcfgd is currently running, and then prints out a message. If there is a running copy, the command returns a 0. If there is no running copy, the command returns a 1. **Note:** When specifying the `-k` parameter and using a nondefault pid file, the `-p` parameter must also be given to ensure that the signal is sent to the correct symcfgd instance, even if there is only a single symcfgd instance running.
`-l severity`	Logs all messages up to and including the specified severity level. Severity must be one of the following: `none`, `emerg`, `alert`, `crit`, `error`, `warning`, `notice`, `info`, `debug`.
`-p <absolute_path>`	Specifies to use the given process ID (pid) file instead of the default `/var/run/symantec/symcfgd.pid` file. You should always use absolute path names when configuring symcfgd. By default, `/var/run/symantec/symcfgd.pid` stores the process ID (pid) of the currently running copy of symcfgd. When symcfgd is terminated, this file is deleted.

Table 3-5 symcfgd service configuration parameters *(continued)*

Parameter	Description
`-s <absolute_path>`	Sets the working directory that the service runs in. You should always use absolute path names when configuring symcfgd. **Note:** This option typically does not need to be changed from the default value, which is the root directory (/).

Note: If you are using a nondefault pid file, you must give the `-p` parameter when using the `-k` parameter, to send the signal to the correct symcfgd instance, even if there is only a single instance running.

About the symcfgd files

Table 3-6 Description of the symcfgd service files

Service file	Description

`/etc/sysconfig/symcfgd`	This configuration file specifies command-line parameters that are passed to the symcfgd program when it is started with the init.d script. To use this file, you must set the parameters to symcfgd between the quotes in the following line:
	`SYMCFGD_OPTS=""`
	For example, to log to the local0 facility and only log up to the error level of severity, you would use the following:
	`SYMCFGD_OPTS="-f local0 -l error"`

`/usr/etc/rc.d/init.d/symcfgd`	This file is the symcfgd startup and shutdown script. This script supports the expected init.d commands, such as `start`, `stop`, `restart`, and so on. The chkconfig command is used to enable or disable the automatic startup of the symcfgd daemon.
`/var/run/symantec/symcfgd.pid`	This file stores the process ID (pid) of the currently running symcfgd. When the currently running symcfgd service is terminated, this file is deleted.

Using the symcfgd service parameters

You can check to see if symcfgd is running, stop symcfgd gracefully, and start it up again.

Note: You must have root privileges to use symcfgd.

You should typically use the /etc/init.d/symcfgd initialization script to perform most tasks that involve the symcfgd service. Using the initialization script ensures that any parameters you have set are picked up when you interact with the service.

Note: Different Linux distributions may have slightly different paths to the startup script directory, but for interoperability, the path /etc/init.d/ should always resolve to the correct startup script directory.

Verifying that the symcfgd service is running

You can use the /etc/init.d/symcfgd initialization script to verify that the rtvscand service is running. Be sure to specify the absolute path to the script.

To verify that the symcfgd service is running

- From the command line, type the following:

```
/etc/init.d/symcfgd status
```

Stopping and starting the symcfgd service

You may want to stop the symcfgd service temporarily. When using the /etc/init.d/symcfgd initialization script, be sure to specify the absolute path to the script.

To stop the symcfgd service

- From the command line, type the following command:

```
/etc/init.d/symcfgd stop
```

To start the symcfgd service

- From the command line, type the following command:

```
/etc/init.d/symcfgd start
```

Specifying the log facility to use and filtering log messages based on severity

You can use the symcfgd -f parameter to log messages using any of the general purpose Linux syslog facilities. To set this up, you must also configure your /etc/syslog.conf file to specify handling for the facility.

You can use the following facilities: daemon, user, local0, local1, local2, local3, local4, local5, local6, and local7. The default facility is daemon.

You can use the `symcfgd -l` parameter with a severity level to filter the messages that are logged. <level> must be one of the following: `none`, `emerg`, `alert`, `crit`, `error`, `warning`, `notice`, `info`, or `debug`. The default level is `info`.

Messages up to and including the specified severity level are logged. For example, if you specify crit, only the messages that are labelled emergency, alert, and critical are logged.

For more information about how you can use these parameters, you can refer to the logger(1), syslog(3), and syslogd(8) man pages on your Linux computer.

About customizing symcfgd

The symcfgd defaults on Linux should work with no changes in any environment. However, if your environment requires that you use a custom initialization script to accommodate specialized functionality, you can use the service parameters from the command line.

Use the following syntax from the command line:

```
symcfgd [-h] [-f log_facility] [-k shutdown|check] [-l severity] [-p
pid_file] [-s path]
```

You must have root privileges to use the symcfgd command-line interface.

About the rtvscand service

The rtvscand service is the interface to rtvscan. rtvscan is the Symantec AntiVirus service that protects Linux client computers from viruses and other security risks. rtvscand performs scans of the file system at the request of Auto-Protect and users.

This service is typically started automatically by the system initialization scripts. No changes to the default values should be required.

About the rtvscand service configuration parameters

The rtvscand parameters are used by the `/etc/sysconfig/rtvscand` file, but can also be used from the command line if special handling is required.

Table 3-7 rtvscand service configuration parameters

Parameter	Description
`-f <log_facility>`	Specifies the log facility to use when logging to syslog. Possible arguments are as follows: ■ `daemon` (default) ■ `user` ■ `local0` through `local7` To set this up, you must also configure your `/etc/syslog.conf` file to specify handling for the facility.
`-h`	Displays help information.
`-k shutdown | check`	Sends a specified signal to the running copy of rtvscand, and then exits. The running copy is identified as the process that has the pid that matches the pid stored in the pid file. This parameter has the following arguments: ■ `Shutdown` sends a signal to shut down the running copy. The process attempts to perform a graceful shutdown. ■ `Check` determines if rtvscand is currently running and prints out a message. If there is a running copy, the command returns a 0. If there is no running copy, the command returns a 1. **Note:** When specifying the `-k` parameter and using a nondefault pid file, the `-p` parameter must also be given to ensure that the signal is sent to the correct rtvscand instance, even if there is only a single rtvscand instance running.
`-l severity`	Logs all messages up to and including the specified severity level. Severity must be one of the following: `none, emerg, alert, crit, error, warning, notice, info, debug`. The default level is `info`.
`-p <absolute_path>`	Specifies to use the given process ID (pid) file instead of the default `/var/run/symantec/rtvscand.pid` file. You should always use absolute path names when configuring rtvscand. By default, `/var/run/symantec/rtvscand.pid` stores the process ID (pid) of the currently running copy of rtvscand. When rtvscand is terminated, this file is deleted.
`-s <absolute_path>`	Sets the working directory that the service runs in. You should always use absolute path names when configuring rtvscand. **Note:** This typically does not need to be changed from the default, which is the root directory (/).

Note: If you are using a nondefault pid file, you must give the `-p` parameter when using the `-k` parameter, to send the signal to the correct rtvscand instance, even if there is only a single instance running.

About the rtvscand files

Table 3-8 Description of the rtvscan service files

File	Description

`/etc/sysconfig/rtvscand`	This configuration file specifies command-line parameters that are passed to the rtvscand program when it is started with the init.d script. To use this file, you must set the parameters to rtvscand between the quotes in the following line:
	`RTVSCAND_OPTS=""`
	For example, to log to the local0 facility and only log up to the error level of severity, you would use the following:
	`RTVSCAND_OPTS="-f local0 -l error"`

`/usr/etc/rc.d/init.d/rtvscand`	This file is the rtvscand startup and shutdown script. This script supports the expected init.d commands, such as `start`, `stop`, `restart`, and so on. The `chkconfig` command is used to enable or disable the automatic startup of the rtvscand daemon.
`/var/run/symantec/rtvscand.pid`	This file stores the process ID (pid) of the currently running rtvscand. When the currently running rtvscand service is terminated, this file is deleted.

Using the rtvscand service parameters

You can check to see if rtvscand is running, stop rtvscand gracefully, change its working directory, and change the file that is used to store the PID of the running copy of rtvscand.

Note: You must have root privileges to use rtvscand.

Although you can use the parameters from the command line, you should typically use the `/etc/init.d/rtvscand` initialization script to perform most tasks that involve the rtvscand service. Using the initialization script ensures that any parameters that you have set are picked up when you interact with the service.

Note: Different Linux distributions may have slightly different paths to the startup script directory, but for interoperability, the path `/etc/init.d/` should always resolve to the correct startup script directory.

Verifying that the rtvscand service is running

You can use the `/etc/init.d/rtvscand` initialization script to verify that the rtvscand service is running. Be sure to specify the absolute path to the script.

To verify that the rtvscand service is running

◆ From the command line, type the following:

```
/etc/init.d/rtvscand status
```

Stopping the rtvscand service

You may want to stop the rtvscand service temporarily. If you do, you should restart rtvscand as soon as possible to protect the computer, because many risks can go undetected when rtvscand is not running. You can use the `/etc/init.d/rtvscand` initialization script to stop the rtvscand service. Be sure to specify the absolute path to the script.

To stop the rtvscand service

◆ From the command line, type the following:

```
/etc/init.d/rtvscand stop
```

Starting the rtvscand service

You can restart rtvscand by running the rtvscand startup script. Be sure to specify the absolute path to the script.

Note: Different Linux distributions may have slightly different paths to the startup script directory, but for interoperability, the path `/etc/init.d/` should always resolve to the correct startup script directory.

The symcfgd service must be running for rtvscand to operate. If you are using the default /etc/init.d/rtvscand script to start rtvscand, the script will check to see if symcfgd is running and start symcfgd if it is not currently running.

To start the rtvscand service

◆ From the command line, type the following:

```
/etc/init.d/rtvscand start
```

Specifying the log facility to use and filtering log messages based on severity

You can use the `rtvscand -f` parameter to log messages using any of the general purpose Linux syslog facilities. To set this up, you must also configure your `/etc/syslog.conf` file to specify handling for the facility.

You can use the following facilities: `daemon, user, local0, local1, local2, local3, local4, local5, local6`, and `local7`. The default is facility `daemon`.

You can use the `rtvscand -l` parameter with a severity level to filter the messages that are logged. <level> must be one of the following: `none, emerg, alert, crit, error, warning, notice, info`, or debug. The default level is `info`.

Messages up to and including the specified severity level are logged. For example, if you specify `crit`, only the messages that are labeled `emergency`, `alert`, and `critical` are logged.

For more information about how you can use these parameters, you can refer to the logger(1), syslog(3), and syslogd(8) man pages on your Linux computer.

About customizing the rtvscand service

The rtvscand service default values should work in any Linux environment. However, if your environment requires that you use a custom initialization script to accommodate specialized functionality, you can use the service parameters to make changes from the command line.

Use the following syntax for the rtvscand command line:

```
rtvscand [-h] [-f log_facility] [-k shutdown|check] [-l severity]
[-p pid_file] [-s path]
```

Note: You must have root privileges to use rtvscand.

About the savtray program

The savtray program is a Symantec AntiVirus graphical user interface tool for viewing Symantec AntiVirus status, program, scan engine, and virus and security risk definitions versions; notifying you of risk events; and starting a LiveUpdate session on the computer.

In the KDE and Gnome desktop environments, Symantec AntiVirus for Linux provides a yellow shield icon on the status tray. 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.

The user interface allows users to do the following:

- Display status and version information, including the version of the program, scan engine, and virus definitions that are in use.
- View risk information found by Auto-Protect or by a scan, if the user has read permission in the directory where the risk was found. If more than one risk is found, users can page through the information.
- Perform LiveUpdates from the status window, unless you have configured Symantec AntiVirus to not allow users to run LiveUpdate.

About savtray command-line syntax

You can use the following syntax for the savtray command line:

```
savtray [-bg color|-background color] [-btn color|-button color]
[-cmap] [-display display] [-fg color|-foreground color] [-fn
font|-font font] [-geometry geometry] [-name name] [-ncols count]
[-reverse] [-session[=]session] [-style[=]style] [-title title]
[visual TrueColor] [-widgetcount]
```

About savtray parameters

These parameters can be used to configure the savtray user interface.

Table 3-9 savtray parameters

Parameter	Description

`-bg <color>`
`-background <color>`
	Sets the default background color and an application palette. Light and dark shades are calculated.

`-btn <color>`
`-button <color>`
	Sets the default button color.

`-cmap`	Causes the application to install a private color map on an 8-bit display.
`-display <display>`	Specifies the name of the X server to use. The default is `$DISPLAY`.

`-fg <color>`
`-foreground <color>`
	Sets the default foreground color that is used for text and graphics.

Table 3-9 savtray parameters *(continued)*

Parameter	Description

`-fn <font>`
`-font <font>`
	Defines the application font. The font should be specified using an X logical font description.

`-geometry <geometry>`	Specifies the initial size and location of the window.
`-name <name>`	Sets the application name.
`-ncols <count>`	Limits the number of colors that are allocated on an 8-bit display.
`-reverse`	Causes text to be formatted for right-to-left languages rather than for left-to-right languages.

`-session=<session>`
`-session <session>`
	Restores the application from an earlier session.

`-style=<style>`
`-style <style>`
	Sets the application GUI style. Possible values are motif, windows, and platinum.

`-title <title>`	Sets the application caption.
`-visual TrueColor`	Forces the application to use a TrueColor visual on an 8-bit display.
`-widgetcount`	When the program exits, prints a debug message that states the number of widgets left undestroyed and the maximum number of widgets that existed simultaneously.

About event notifications

If a user is using a KDE or Gnome environment with the savtray package installed, they will get notifications of events under some circumstances.

If a user's action, such as opening a file, triggers the detection of a risk, the user will get a notification dialog box from Auto-Protect. On multi-user machines, users will see a notification only if their own action triggered the detection of the risk. Since only users with root privileges can run manual and scheduled scans, most users will never see notifications of risks that are found by these scans.

Users with root privileges will get a notification dialog box if risks are found during a manual scan or scheduled scan while they are logged on. They will also see a notification dialog box when Auto-Protect detects a risk that is triggered by one of their actions.

All generated events are logged to the standard system log via syslog, regardless of which user triggers their detection and whether Symantec AntiVirus detects them via Auto-Protect or a manual or scheduled scan.

Updating virus definitions on Linux

This chapter includes the following topics:

About updating virus definitions on Linux

You can update the virus and security risk definitions on your Linux client computers in the following ways:

- Use the LiveUpdate Administration Utility, LuAdmin, to set up a Central LiveUpdate server on your network. Configure Java LiveUpdate to point your clients to pick up definitions updates from that server.
- Use an Intelligent Updater shell script.
- Initiate a manual LiveUpdate from the user interface or command line on the computer.
  Users can update the virus definitions on a computer that uses LiveUpdate from the user interface or the command line. Or you can configure the `GRC.DAT` file not to allow this.

Note: The definitions file and Intelligent Updater script that are used for Linux computers are not the same as the definitions file and Intelligent Updater script that are used on Windows computers.

See "About the LiveUpdate Administration utility" on page 58.

See "Updating definitions by using Intelligent Updater" on page 68.

About the LiveUpdate Administration utility

The LiveUpdate Administration utility, `luau.exe`, is a self-extracting compressed archive that lets you download update packages and configure clients to retrieve those updates from an internal proxy server. It is used to set up a central LiveUpdate server on your internal network. Rather than all client computers contacting the Symantec servers to obtain definitions and product updates, the client computers contact a Central LiveUpdate server on your local network.

Note: You must install and run LuAdmin on a Windows 2000 Professional/2003/XP Professional 32-bit, SP2 computer. LuAdmin is not available for Linux computers.

Using a Central LiveUpdate server means that clients do not need to connect to an external network for virus definitions and product updates. This reduces WAN traffic and transfer speeds for clients in the network that do not have access to the Internet. It also allows updating definitions for unmanaged clients and lets you manage bandwidth usage for definitions updates by scheduling when LiveUpdate runs. In addition, using a Central LiveUpdate server gives you control over the types of updates that are available to users.

You can use LuAdmin to perform the following tasks:

- Select the Symantec products and languages for which updates are downloaded.
- Specify the full path to the directory in which downloads are stored.
- Retrieve all of the update packages and related index files from the Symantec LiveUpdate site that apply to the selected products.

LuAdmin is typically installed on one computer on the network. LuAdmin does not need to be installed on the same server that is used as the Central LiveUpdate server. If you set up the Central LiveUpdate server on a separate computer, then you can test new updates before moving them to the Central LiveUpdate server.

Warning: The LuAdmin packages that are downloaded can be large, so Symantec does not recommend this method for networks with slow Internet connections, especially dial-up connections.

About LuAdmin files

The files that you need to install and use LuAdmin are located on the Symantec AntiVirus Win32 product discs in the `\Tools\LiveUpdate` directory. You need the following files:

- `LUAESD.exe`, the LuAdmin Utility
- The *LiveUpdate Administrator User's Guide*

Note: If you already have the latest version of LuAdmin installed on a computer in your network, you do not need to install the copy that is provided with this product.

Note: For information about installing LuAdmin, setting up a central LiveUpdate server, and downloading updates, refer to the *LiveUpdate Administrator User's Guide*.

About Java LiveUpdate

Java LiveUpdate is the Symantec technology that provides LiveUpdate services on Windows server products and non-Win32 operating systems, such as Linux.

Java LiveUpdate functions similarly to the Win32 version of LiveUpdate. When Java LiveUpdate runs, it connects to the server that is specified in the host file or in the liveupdate.conf file.

Java LiveUpdate determines if there are updates available for the specified products. For each update that is found, a temporary directory is created under the local package directory into which the zipped files are copied. The packages are authenticated, unzipped, and installed. The temporary directory and files are then removed.

Java LiveUpdate tracks configuration information about multiple LiveUpdate servers or hosts. It tries each of the servers in the order in which they are listed in the Java LiveUpdate configuration file, and automatically fails over to the next host if it finds that the server is unreachable.

About the Java LiveUpdate configuration file

By default, Java LiveUpdate gets its configuration information from the liveupdate.conf file. The liveupdate.conf file on Linux is located in /etc.

Table 4-1 describes the parameters that you can set when you configure Java LiveUpdate.

Table 4-1 `liveupdate.conf` file parameters

Parameter	Description
`workdir`	The working directory on the client computer. This entry is required. Java LiveUpdate creates a local package directory under the specified working directory. If the working directory does not exist, Java LiveUpdate creates it and uses the working directory as the local package directory.
`logfile`	The full path to the log file that Java LiveUpdate uses to log events and errors. If this setting is omitted, no log file is created.
`jar`	The full path to the jlu.jar file. If this file is omitted, Java LiveUpdate looks for its JAR file in the LiveUpdate subdirectory immediately under the Symantec directory. The location of the Symantec directory is specified by the BaseDir parameter in the Symantec Shared section of the Symantec global configuration file /etc/Symantec.conf. Java LiveUpdate returns an error immediately if it cannot locate its JAR file.
`urls`	The URLs of external Symantec server support. By default, Java LiveUpdate ignores the URL= lines in the TRI file. If this parameter is 1 (true), Java LiveUpdate uses the URL= lines in the TRI file when it uses HTTP to download packages. This parameter and the URL= lines are ignored if FTP is specified as the protocol.
`proxy`	The name of a proxy server. For example: proxy=addr:port, where the port number is optional. The default port is 80. Addr is the TCP/IP address of the proxy server and :port is the TCP/IP port on which the proxy server is listening (optional). This setting is not supported for FTP.
`proxyusername`	The user name to use when you log on to the specified proxy server. This setting is needed only if your proxy server requires a logon user name. This setting is not supported for FTP.
`proxypassword`	The password that is associated with the specified proxyusername account. This setting is needed only if your proxy server requires a logon password. This setting is not supported for FTP.
`maximumLogFileSize`	The maximum allowed log file size, in kilobytes (KB). Java LiveUpdate discards older log entries once the log file exceeds the specified maximum size. The default log file size is 1024 KB.

Table 4-1 `liveupdate.conf` file parameters *(continued)*

Parameter	Description
`AllowConfigurationOverride`	The setting that is used to tell Java LiveUpdate to use the -c command-line parameter and host file setting. If this parameter is set to anything other than True in the shared liveupdate.conf file, Java LiveUpdate ignores the -c parameter and host file setting.
`hosts/<host#>/url`	The URL of a LiveUpdate server. You may specify a nonstandard port for HTTP servers and a package directory for both FTP and HTTP servers. Java LiveUpdate supports up to 10 servers, starting with 0 through 9. This setting replaces the following Java LiveUpdate 1.10 settings: ■ `protocol` ■ `host` ■ `packagedir` ■ `login` ■ `password`
`hosts/<host#>/access`	The local directory or mapped directory to access for updates. The path may be a full local path or a UNC share.
`hosts/<host#>/login`	The user name to use when logging on to a LiveUpdate server using FTP. This optional setting is ignored for all other transports.
`hosts/<host#>/password`	The password to use when logging on to a LiveUpdate server using FTP. This optional setting is ignored for all other transports.
`ConnectionTimeout`	The connection time in milliseconds that Java LiveUpdate waits when it attempts to connect to a LiveUpdate server. The default is 60000 (60 seconds).
`ConnectionReadTimeout`	The connection timeout in milliseconds that Java LiveUpdate waits for responses from the LiveUpdate server once a connection has been established. The default is 30000 (30 seconds).
`extlog/host#/url=syslog: //<address>[:<port>]`	The host address and port of the system log to which Java LiveUpdate sends logs.
`extlog/host#/url=sgs`	The URL that is used to send logs to Symantec Gateway Security (SGS). This entry may be included only one time in the configuration file.
`extlogdest=extlog host#[,extlog/host#]`	The list of active external logging services. This setting enables specified external logons if the list is not empty.
`enableSyslogLocalization`	The parameter that determines whether to enable localized messages in the syslog. If this parameter is set to `YES`, localized messages are enabled. The default is `NO`.

You must specify the working directory on the client computer using the `workdir` parameter.

Java LiveUpdate must also be able to find its JAR file. For UNIX platforms, Java LiveUpdate searches for `jlu.jar` in the LiveUpdate subdirectory immediately under the Symantec directory that is specified in `/etc/Symantec.conf`.

If you want to use a legacy host file, you must type the full path to the host file. The only parameters that are required in the configuration file are the workdir and the hostfile settings. If you are not using a legacy host file, the workdir and the `hosts/<host#>/url` setting must be specified.

If a setting is followed by :ENC, the value has been encrypted by Java LiveUpdate. The settings that may be encrypted are as follows:

- `login`
- `password`
- `proxyusername`
- `proxypassword`
- `hosts/<host#>/login`

Java LiveUpdate 2.0 and later automatically encrypts the login and password settings each time that Java LiveUpdate runs, if the :ENC tag is missing.

Sample liveupdate.conf file

Following is an example of a liveupdate.conf file on UNIX using Java LiveUpdate 2.0 or later:

```
hosts/0/url=http://liveupdate.symantecliveupdate.com:80
hosts/1/url=http://liveupdate.symantec.com:80
hosts/2/login:ENC=b3effee10d982d2c7449c810c
hosts/2/password:ENC=19d3d3v3c123333898dcf293d
hosts/2/url=ftp://update.symantec.com/opt/content/onramp
workdir=/tmp
logfile=/opt/Symantec/LiveUpdate/liveupdt.log
jar=/opt/Symantec/LiveUpdate/jlu.jar
urls=1
proxy=proxy.yourcompany.com:8080
proxyusername=joe
proxypassword=geer132
maximumLogFileSize=512
AllowConfigurationOverride=true
```

About configuring proxy settings in Java LiveUpdate

You can configure proxy settings for Java LiveUpdate by changing the following line in the `/etc/liveupdate.conf` file:

```
proxy=proxy.yourcompany.com:8080
```

To use authentication, you can also edit the following proxyusername and proxypassword lines:

```
proxyusername=MyCompany_user_name

proxypassword=MyCompany_password
```

Configuring Java LiveUpdate to use a Central LiveUpdate server

To set up a Central LiveUpdate server, you need do the following:

- Install LuAdmin.

  Note: You must install and run LuAdmin on a Windows 2000 Professional/ 2003/XP Professional 32-bit, SP 2 computer. It is not available for Linux computers.

- Configure LuAdmin to download the definitions from Symantec onto a Central LiveUpdate server on your network.

  Note: Choose **Symantec AntiVirus Virus Definitions** under **Symantec Product Line** when picking the updates to download in LUAdmin.

- Modify a copy of the `liveupdate.conf` file to point to your Central LiveUpdate server. You can specify an internal FTP or HTTP server.
- Use any file distribution mechanism to replace the `/etc/liveupdate.conf` file on each of your Linux client computers with your modified file.

You can configure Java LiveUpdate to use a Central LiveUpdate server by changing one line in the `/etc/liveupdate.conf` file. You should edit the `/hosts/0` line so that the first server that is checked by your clients is your Central LiveUpdate server.

After you have edited one liveupdate.conf file, use any file distribution mechanism to replace the existing /etc/liveupdate.conf file on all your Linux client computers.

To configure the liveupdate.conf file to use a Central LiveUpdate server

- In the liveupdate.conf file, edit the following line to specify the full path to the update definitions directory on your central LiveUpdate server:

  hosts/0/url=<full path to the update definitions directory on the central LiveUpdate server>

  Be sure to change the hosts/0/ line so that the first place the client checks for updates is your central server.

For information on installing and configuring LuAdmin, see the *LiveUpdate Administrator User's Guide*.

Wrapping a liveupdate.conf file in an rpm package

If you want to distribute a liveupdate.conf file to all your Linux computers, you can wrap the liveupdate.conf file in an rpm package. Symantec provides a script called make_luconf_rpm.sh and its associated file, luconf.spec, to automate this process. The files are located in the luconfrpm directory.

After you have wrapped the liveupdate.conf file into an rpm package, you can use your rpm distribution to put the liveupdate.conf file into the /etc directory on the Linux computers.

Note: make_luconf_rpm.sh creates an rpm package with the same version number every time. The first time that you run the script, the package installs. Each subsequent time that you run the script and attempt to install it, the rpm package does not install because its version number indicates that this package is already installed.

Each time that you run this script after the first time, you’ll need to do one of the following to get the package to install:

- Force the installation using the rpm --force option.
- Edit the luconf.spec script and increment the minor macro number, %define minor, by one.

When you use rpm to install a new liveupdate.conf file that is produced by using this script, rpm first checks to see if there is an existing liveupdate.conf file on the computer. If there is, rpm makes a copy of the file and names it liveupdate.conf.rpm.orig. If you use rpm to uninstall this package, rpm uninstalls the file by changing its name to liveupdate.conf.rpm.save.

To wrap a liveupdate.conf file in an rpm package

1 Create a liveupdate.conf file or edit an existing one.

2 Copy the make_luconf_rpm.sh file from the luconfrpm directory on the Symantec product disc or in your download location to the location where you want to package the liveupdate.conf file. Alternatively, you can copy the file onto a DVD and use the /var/tmp directory. You must have write and execute permissions in the directory where you wrap the file.

3 At the command line, type the following:

```
<absolute_path>/make_luconf_rpm.sh <absolute_path>/
liveupdate.conf
```

When you type this command, you must use the fully qualified path for the liveupdate.conf file, even if it is located in the same directory as the script. For example, if you have both the script and the liveupdate.conf file in the same directory and you are in that directory, you can type the following:

```
$PWD/make_luconf_rpm.sh $PWD/liveupdate.conf
```

The file that is created is named luconf-1.0.1-1.noarch.rpm. It is placed in the root of the current directory.

Enabling Java LiveUpdate logging on Linux servers

By default, a Linux syslog server is not configured to receive messages from remote clients.

To receive Java LiveUpdate messages, you must do the following:

- Create an entry in syslog.conf for logging Java LiveUpdate messages.
- Create a messages log file.
- Configure the syslog startup options.

If the syslog server is different from the server that runs Java LiveUpdate, you must modify the firewall to allow inbound traffic on port 514. Finally, you must restart the server for the changes to take effect.

Note: Use tabs and not spaces when you editing the line in the /etc/syslog.conf configuration file.

To create an entry in `syslog.conf` for logging Java LiveUpdate messages

- In the `/etc/syslog.conf` configuration file, type **`local0.*`**, and then type the file that you want to send the messages to.

  For example:

  ```
  local0.* /var/log/jlu.log
  ```

  Do not use spaces between local0.* and the name of the file. Use tabs to separate the expressions.

To create a jlu.log file

- At the command line, type the following:

  ```
  touch /var/log/jlu.log
  ```

See "Configuring startup options" on page 66.

Configuring startup options

Syslog checks the `/etc/syslog.conf` file to determine the expected names and locations of the log files that it creates. It also checks the `/etc/sysconfig/syslog` to determine the various modes in which it should operate. Syslog listens for remote messages when you add the variable -r to SYSLOGD_OPTIONS and -x to disable DNS lookups on the messages that are received with `-r`.

For example:

Options to syslogd

# `-m 0` disables 'MARK' messages.

# `-r` enables logging from remote machines

# `-x` disables DNS lookups on messages received with **`-r`**

#See **`syslogd(8)`** for more details

`SYSLOGD_OPTIONS="-m 0 -r -x"`

`# Options to klogd`

`-2`prints all kernel oops messages twice; once for klogd to decode, and once for processing with 'ksymoops'

`-x` disables all `klogd` processing of `oops` messages entirely Using Java LiveUpdate 11

Enabling Java LiveUpdate logging on Linux servers

See `klogd(8)` for more details **`KLOGD_OPTIONS="-2"`**

Note: Make sure that `SYSLOGD_OPTIONS` contains **`-r -x`**.

Configuring firewall rules in `/etc/sysconfig/iptables`

You must modify your firewall to allow inbound traffic on UDP port 514. To ensure that you receive only legitimate log entries, you should limit `/etc/sysconfig/iptables` to the client systems that send logs to you.

To configure firewall rules in `/etc/sysconfig/iptables`

1. Do one of the following tasks:
   - If you use Linux, start iptables if necessary, and then add the following rule to be used on the logging server, which is the computer that receives syslog messages:

     ```
     -A INPUT -o $IFACE -p udp -s $LOGCLIENT -d $MYIP --dport 514
     -j ACCEPT
     ```

     In this example, `$IFACE` is your external ethernet interface (eth0). `$MYIP` is the IP address of the server to which you add this iptables rule. `$LOGCLIENT` is the IP address of the computer that sends the messages. This rule assumes a default `OUTPUT` policy of `DENY`.
   - If you use Red Hat Linux, manually add the following line to the `/etc/sysconfig/iptables` file:

     ```
     -A RH-Lokkit-0-50-INPUT -p udp -m udp --dport 514 -j ACCEPT
     ```

     This line should precede any reject lines.
2. Confirm that your `iptables` configuration file is owned by user root, group root. For example:

   ```
   chown root:root /etc/sysconfig/iptables
   ```
3. Change the permissions of your `iptables` configuration file to read and write by user root only. For example:

   ```
   chmod 600 /etc/sysconfig/iptables
   ```
4. To allow the changes to take effect, do both of the following:
   - To restart `iptables`, type the following command at the command line:

     ```
     /etc/init.d/iptables restart
     ```
   - To restart `syslog`, type the following command at the command line:

```
/etc/init.d/syslog restart
```

5 To verify that the syslog daemon is running, type the following command:

```
ps -aux | fgrep syslog
```

The output should be similar to the following:

```
root 1662 0.0 0.0 1576 616 ? S Nov09 0:00 syslogd -m 0

root 18738 0.0 0.0 3664 548 pts/0 S 09:34 0:00 grep -F syslog
```

The first line confirms that the syslog daemon process is up and running; the second line is the command.

Verifying syslog messages

You can use `tcpdump` to verify that syslog messages arrive at the server. For example:

```
tcpdump -a -vv -I -p -c 1000 > tcpdump.log
```

This configures Linux to run in promiscuous mode so that it receives all messages, logs in ASCII format with increased verbosity to the tcpdump.log file, and then exits after 1000 packets are logged. You can determine if a problem exists on the syslog side, or if a rule is missing for remote logging on a computer that has a firewall.

To verify syslog messages

◆ At the command line, type the following command:

```
cat tcpdump.log | grep -v "\^" | grep udp
```

This should return values similar to either `. > .514 udp` or `. > .syslog udp`. If no Java LiveUpdate messages are making it to the syslog destination, yet the tcpdump log displays lines similar to `. > .514 udp` or `. > .syslog udp`, the problem must be that something other than that the syslog configuration prevents Java LiveUpdate syslog messages from reaching the syslog target. For example, there may be a firewall on the syslog computer that blocks the syslog port.

Updating definitions by using Intelligent Updater

Rather than updating virus and security risk definitions by using LiveUpdate on each Linux client computer, you can download an Intelligent Updater shell script. The script has a name in the format `yyyymmdd-version-unix.sh`, such as `20050601-008-unix.sh`.

The latest Intelligent Updater script is located on the Symantec Security Response Web site at the following URL:

http://securityresponse.symantec.com/avcenter/defs.download.html

For Linux, this script depends on the utilities that are distributed as part of the UNIX sharutils package, which must be installed on the computer. It also relies on the UNIX uncompress utility, which is not available on some Linux distributions. If your distribution does not have uncompress, you can work around this issue by creating a symbolic link to the functionally equivalent zcat utility.

Note: The Symantec AntiVirus Linux client computers poll for new definitions every 10 minutes. Alternately, you can prompt Symantec AntiVirus to check immediately for new definitions by using symcfg to set the `\Symantec Endpoint Protection\AV\ProductControl\NewPatternFile` key to **1**.

Downloading and running the Intelligent Updater script

To use Intelligent Updater, you need to download and run the script.

To download the script

1. Go to the **Symantec Security Response Virus Definitions Download Page** at the following URL:

   http://securityresponse.symantec.com/avcenter/defs.download.html

2. Select the appropriate language.

3. Select **Virus Definitions** under **File-Based Protection (Traditional Antivirus)** as the product.

4. Scroll down to **Unix Platforms**, right-click the file listed under the **File Name** heading, and save it to your computer.

To run the script

1. With the file on the appropriate Linux computer, change the file's permissions to make it executable. For example, type the following:

   ```
   chmod 755 *unix.sh
   ```

2. Double-click the file to run it, or run it from the command line.

   The script then puts the new definitions into the `/opt/Symantec/virusdefs/incoming` directory.

Configuring Symantec AntiVirus for Linux

This chapter includes the following topics:

About configuring Linux clients using a `GRC.DAT` file

You can configure Linux client computers using a `GRC.DAT` file and the Configuration Editor.

If you have an unmanaged Symantec environment, you use the Configuration Editor tool on a Windows computer that has Symantec AntiVirus installed to create and deploy a `GRC.DAT` file. You copy the `GRC.DAT` file directly to your Linux client computers or wrap the `GRC.DAT` file in an rpm package for distribution.

A subset of the configuration settings that are available in the Configuration Editor tool are supported on Linux computers.

See "Deploying `GRC.DAT` files to Linux client computers" on page 79.

About the Configuration Editor tool

The configuration file (`GRC.DAT`) is the heart of the communication between the following components:

- Symantec Client Security server and client
- Symantec AntiVirus server and client
  If you have an unmanaged Symantec product deployment, you can manage your Symantec AntiVirus Linux client computers.

Configuration files store information such as parent server identity and antivirus server and client configuration settings.

You can use the Configuration Editor (`Configed.exe`) to generate a configuration file that can be used with Symantec Client Security server and client or Symantec AntiVirus server and client.

With the Configuration Editor, you can create different configurations that can be distributed to clients at any time. For example, an administrator of an organization with the separate server groups that are set up for departments with different security needs can create a configuration file with different settings for each of the server groups.

Note: The Configuration Editor does not support creating `Grcgrp.dat` and `Grcgrpl.dat` files.

The Configuration Editor tool is located with this product in the `\Tools` directory.

Note: You must run the Configuration Editor on a Windows computer that has Symantec AntiVirus installed.

See “Opening the Configuration Editor” on page 72.

Opening the Configuration Editor

To start using the Configuration Editor, you need to copy the program from the installation product disc onto a Windows desktop. You can then launch it.

To open the Configuration Editor

1. On the installation product disc or the installation download location, click the **SAVLINUX** > **Tools** folder.
2. Copy `Configed.exe` to your Windows desktop.
3. On your Windows desktop, double-click the **Configed** icon.

See "Creating a configuration file" on page 73.

Creating a configuration file

To create a new configuration file, you first modify settings in the Configuration Editor and then save the file as a new `GRC.DAT` file.

To create a configuration file

1. Open the Configuration Editor.

   See "Opening the Configuration Editor" on page 72.
2. In the main Configuration Editor window, click the settings you want to configure.
3. When you have finished setting all of the settings, click **Save GRC.dat**.
4. Locate the directory to which you want to save the file, and click **Save**.

You must name the file `GRC.DAT`, all in capital letters and place the `GRC.DAT` file in the appropriate client directory before it is processed:

```
/var/symantec
```

Modifying an existing configuration file

To change the settings in an existing `GRC.DAT` file, complete the following tasks:

- Locate and load the existing GRC.DAT file.
- Change the configuration settings.
- Save the file.

To modify an existing configuration file

1. Open the Configuration Editor, and click **Load GRC.dat.**
2. Locate the existing `GRC.DAT` file, select it, and click **Open**.
3. Change the settings.

4. Click **Save GRC.dat**.
5. Locate the directory to which you want to save the file, and click **Save**.

   You must name the file `GRC.DAT`, all in capital letters and place the `GRC.DAT` file in the appropriate client directory before it is processed:

   `/var/symantec`

Returning settings to their default configuration

At any time while you create or edit a `GRC.DAT` file, you can return all settings to their defaults.

To return all settings to their default configuration

◆ In the main Configuration Editor window, click **Reset Options**.

About the settings in the `GRC.DAT` file

The locking of configuration settings is not supported on Linux. By default, a user must have root privileges to make local configuration changes on a Symantec AntiVirus Linux client computer.

Note: Scanning for security risks is not enabled by default in Symantec AntiVirus for Linux. You can enable security risk scans by using the `GRC.DAT` file. Security risks are then detected and logged, but Symantec AntiVirus cannot take any actions on them.

For scheduled scans, scanning for security risks is set separately for each scheduled scan in the **Scan Options** dialog box. For manual scans, set this option for a single scan to run when the new `GRC.DAT` file is processed by checking **Configure client to run a manual scan on GRC.DAT file processing**. You can set the option as the default for all subsequent manual scans by unchecking **Configure client to run a manual scan on GRC.DAT file processing**.

Table 5-1 describes the supported configuration settings for Linux computers and their locations in the Configuration Editor.

Table 5-1 Supported configuration settings for Linux clients

Setting category	Supported configuration settings	Location
Tray icon	Show Symantec AntiVirus icon on desktop	Not available.

Table 5-1 Supported configuration settings for Linux clients *(continued)*

Setting category	Supported configuration settings	Location
File System Auto-Protect	Enable Auto-Protect Scan file types by extension Scan for Security Risks Exclude selected files and folders See "About file extension exclusions" on page 78. Scan Network, Floppy, and DVD-ROM drives	**Client Auto-Protect Options** button, **Client Auto-Protect Options** dialog box
File System Auto-Protect, Advanced Scan options	Scan files when modified Scan files when accessed or modified Disable file cache Use default file cache size Custom file cache entries	**Client Auto-Protect Options** button > **Client Auto-Protect Options** dialog box > **Advanced** button
File System Auto-Protect, Actions	**Actions** tab: First Actions **Actions** tab: Second Actions **Exceptions** tab: Add and configure First and Second actions **Note:** Only the actions for viruses are supported. No actions are supported for security risks.	**Client Auto-Protect Options** button, **Client Auto-Protect Options** dialog box, **Actions** button
File System Auto-Protect, Notifications	Display notification message on infected computer, and the text field for constructing the message	**Client Auto-Protect Options** button > **Client Auto-Protect Options** dialog box > **Notifications** button
Virus Definition Manager	Schedule client for automatic product updates using LiveUpdate Do not allow client to manually launch LiveUpdate	**Virus Definition Manager** button, **Virus Definition Manager** dialog box
Virus Definition Manager, Advanced Schedule Options	Handle missed events within N days of the scheduled time Perform update within plus or minus N minutes of the scheduled time Randomize the day of the week within the interval beginning on <day> and ending <day>	**Virus Definition Manager** button, **Virus Definition Manager** dialog box, **Advanced** button

Table 5-1 Supported configuration settings for Linux clients *(continued)*

Setting category	Supported configuration settings	Location
Scheduled Scans, Scheduled Scans Options	Name Enable scan Frequency When	**Scheduled Scans button, Scheduled Scans** dialog box, **New** or **Edit** buttons
Scheduled Scans, Scan Options	File types: All types File types: Selected extensions, Extensions button Enable detection of security risks Exclude files and folders: Exclusion button See "About file extension exclusions" on page 78.	**Scheduled Scans** button, **Scheduled Scans** dialog box, **New** or **Edit** buttons, **Scan Settings** button
Scheduled Scans, Scan Advanced Options	Scan files inside compressed files If there is a compressed file within a compressed file, expand: N levels deep	**Scheduled Scans** button, **Scan Options** dialog box, **New** or **Edit** buttons, **Advanced** button
Scheduled Scans, Actions	**Actions** tab: First Actions **Actions** tab: Second Actions **Exceptions** tab: Add and configure First and Second actions **Note:** Only the actions for viruses are supported. No actions are supported for security risks.	**Scheduled Scans** button, **Scheduled Scans** dialog box, **New** or **Edit** buttons, **Actions** button
Scheduled Scans, Notifications	Display notification message on infected computer Text field for constructing the message	**Scheduled Scans** button, **Scheduled Scans** dialog box, **New** or **Edit** buttons, **Notifications** button
Scheduled Scans, Advanced Schedule Options	Handle missed events within N days of the scheduled time	**Scheduled Scans** button, **Scheduled Scans** dialog box, **New** or **Edit** buttons, **Advanced** button

Table 5-1 Supported configuration settings for Linux clients *(continued)*

Setting category	Supported configuration settings	Location
Manual Scans, Immediate Manual Scan Options	Configure clients to run a manual scan on `GRC.DAT` file processing Check this option to restrict the settings you configure using the Settings button to a single scan to be run as soon as the new `GRC.DAT` file is processed. Uncheck this option to make the settings you configure using the Settings button the default for all subsequent manual scans.	**Immediate Manual Scan** button
Manual Scans, Immediate Manual Scan Options, Settings button	File types: All types File types: Selected extensions, Extensions button Enable detection of security risks Exclude files and folders: Exclusion button See "About file extension exclusions" on page 78.	**Immediate Manual Scan** button, **Settings** button
Manual Scans, Scan Advanced Options	Scan files inside compressed files If there is a compressed file within a compressed file, expand: N levels deep	**Immediate Manual Scan** button, **Settings** button, **Advanced** button
Manual Scans, Actions	**Actions** tab: First Actions **Actions** tab: Second Actions **Exceptions** tab: Add and configure First and Second actions **Note:** Only the actions for viruses are supported. No actions are supported for security risks.	**Immediate Manual Scan** button, **Settings** button, **Advanced** button, **Actions** button
Manual Scans, Notifications	Display notification message on infected computer Text field for constructing the message	**Immediate Manual Scan** button, **Settings** button, **Advanced** button, **Notifications** button

Note: All other settings in a `GRC.DAT` file are ignored or unsupported on Linux computers running Symantec AntiVirus.

About file extension exclusions

In previous versions of the Configuration Editor tool, file extensions were automatically capitalized to normalize the data for case-insensitive platforms such as Windows and NetWare.

Note: You must edit the `GRC.DAT` file manually to add lowercase or mixed-case file extension exclusions to `GRC.DAT` files that you produced using the Configuration Editor from Symantec AntiVirus 10.0 or earlier. If you use the Configuration Editor from Symantec AntiVirus 10.1 or later, no manual editing is required.

As there is no version information in the Configuration Editor, the only way to determine which version you use is to know which version of Symantec AntiVirus you obtained it from.

File extension exclusions should be added to the Exts value in the appropriate scan settings section. For example, to add the extensions xxx and zzz as exclusions to the scheduled scan named My Linux Scan, you add the text xxx,zzz in the following location:

```
!KEY!=$REGROOT$\LocalScans\ClientServerScheduledScan_XX

...

Exts=Sxxx,zzz

...

ExcludedByExtensions=D1

...

StatusDialogTitle=SMy Linux Scan

...

!KEY!=$REGROOT$\...
```

To add the extensions xxx and zzz as exclusions for Auto-Protect, you add the text xxx,zzz in the following location:

```
!KEY!=$REGROOT$\Storages\FileSystem\RealTimeScan

...

Exts=Sxxx,zzz

...

ExcludedByExtensions=D1
```

```
...
!KEY!=$REGROOT$\...
```

Deploying GRC.DAT files to Linux client computers

GRC.DAT files are text files that you can edit manually using a text editor or the Configuration Editor. Symantec AntiVirus Linux client computers support GRC.DAT files with either Windows or Linux line endings. The file may not be in Unicode format.

After you create a GRC.DAT file, you can then copy the GRC.DAT file directly to your Linux client computers or wrap the GRC.DAT file in an rpm package for distribution.

GRC.DAT files are automatically imported every 10 minutes. Alternately, administrators can prompt Symantec AntiVirus to import a GRC.DAT file immediately by using the symcfg command line interface to set the value of \Symantec Endpoint Protection\AV\ProductControl\ProcessGRCNow to 1.

Table 5-2 lists the tasks that you need to perform to configure the settings on your Linux client computers by using the GRC.DAT file.

Table 5-2 Deploying the GRC.DAT configuration file

Task	Description
Wrap the GRC.DAT file in an rpm package.	After you create or modify an existing configuration file, you wrap it in an rpm package using a script. The make_grcrpm.sh script and its associated file, grc.spec automates this process. Alternatively, you can copy the file onto a DVD and use the /var/tmp directory. You must have write and execute permissions in the directory where you wrap the file. See "Wrapping a GRC.DAT file in an rpm package" on page 80.
Copy and paste the GRC.dat file to the Linux client computers.	Copy and paste a wrapped rpm package with the modified GRC.DAT file to the Linux client computers. See "Copying a GRC.DAT file" on page 80.
Ensure that the end users install the GRC.DAT file to the Linux client computers.	The user installs the rpm package to a customized installation path with the option prefix. For this type of installation, you must install these rpm packages to the same path. For example, you can type the following command: **rpm -Uhv --prefix *yourpath* *.rpm**.

Wrapping a GRC.DAT file in an rpm package

Note: make_grcrpm.sh creates an rpm package with the same version number every time. The first time that you run the script, the package installs. Each subsequent time that you run the script and attempt to install it, the rpm package does not install because its version number indicates that this package is already installed.

Each time that you run this script after the first time, you'll need to do one of the following to make the package install:

- Force the installation using the rpm --force option.
- Edit the grc.spec script and increment the minor macro number, %define minor, by one.

To wrap a GRC.DAT file in an rpm package

1. With the Configuration Editor, create a GRC.DAT file with the configuration file that you want on a Windows parent server.

   See "Creating a configuration file" on page 73.

2. Copy the make_grcrpm.sh file from the grcrpm directory on the Symantec product disc to the location where you want to package the GRC.DAT file.

3. At the command line, type the following command:

   <absolute_path>/make_grcrpm.sh <absolute_path>/GRC.DAT

   When you type this command, use the fully qualified path for the GRC.DAT file, even if it is located in the same directory as the script.

   For example, if the script and the GRC.DAT file are both in the same directory as you, type the following command:

   $PWD/make_grcrpm.sh $PWD/GRC.DAT

   The file that is created is named grc-1.0.1-1.noarch.rpm. It is placed in the root of the current directory.

Copying a GRC.DAT file

After you have wrapped the GRC.DAT file into an rpm package, use your rpm distribution to put the GRC.DAT file into the /var/symantec directory on the Linux computers.

To copy and paste a `GRC.DAT` file

1. Copy the modified GRC.DAT file from your Windows desktop

   When you copy a `GRC.DAT` file to a Symantec AntiVirus for Linux client computer, make sure that the file name is `GRC.DAT` in capital letters.

2. Paste the configuration file onto a DVD and copy it to the `/var/symantec` directory of the Linux clients.

3. From the command line, type the following command:

   cp <absolute_path>/GRC.DAT <destination_path>

Chapter 6

Using the Symantec AntiVirus for Linux Reporter

This chapter includes the following topics:

About the Symantec AntiVirus for Linux Reporter

The Symantec AntiVirus for Linux Reporter provides log records and inventory information to the Symantec Endpoint Protection Manager by using its legacy reporting channel. You can then monitor and report on SAVFL client activities from the Symantec Endpoint Protection Manager console.

The Reporter forwards the following logs to the Symantec Endpoint Protection Manager:

- Inventory (Computer Status) logs, which include Parent Server Name, Server Group Name, Client Name, Client Group, Product Version, ScanEngine Version, Last Checkin Time, User Name, Virus Definition Date, Virus Definition Sequence, Virus Definition Revision, Virus Definition Version, IsInfected, IP Address, Running Status, AutoProtect OnOff, TimeZone.
- Scan logs, which are generated by Symantec AntiVirus for Linux as logging events.

- Virus (Risk) logs, which are generated by Symantec AntiVirus for Linux as logging events.

Installing the Symantec AntiVirus for Linux Reporter

The Symantec AntiVirus for Linux Reporter is compatible with the following versions of Symantec Endpoint Protection Manager:

- Symantec Endpoint Protection 11 RU5 or earlier
- Symantec Endpoint Protection 11 RU6 MP2 with PP1 or later

To install the Symantec AntiVirus for Linux Reporter:

1 Install Symantec Endpoint Protection Manager.

2 In the Symantec Endpoint Protection Manager console, click **Home > Preferences > Logs and Reports - Legacy Support**, and check **Upload Symantec AntiVirus version 10.x log files**.

Note: You may see a pop-up warning message telling you that there are manual steps needed. Click **Help** on the **Logs and Reports** tab for details on those steps.

3 Install a SAVFL MR10 or later package on the client.

The SAV package is required.

4 Make sure that Perl 5.8.0 or later and the related Perl module package (for example, `perl-libwww-perl` for RedHat/SuSe Linux) are installed on the client.

5 Install the SAVFL reporter package by typing one of the following commands:

`# rpm -Uhv savreporter-*.noarch.rpm` (on RedHat/SuSe Linux); or

`# dpkg -i savreporter-*.all.deb` (on Ubuntu/Debian Linux).

6 Edit the configuration file `/etc/reporterd.ini` to set the server IP address and modify the other settings.

7 Optionally, switch the reporter service to RunNow mode by typing the following command:

```
# /etc/init.d/reporterd runnow
```

You can then see the Scan log, Risk log, and Computer Status log in the Symantec Endpoint Protection Manager console.

Configuring the Symantec AntiVirus for Linux Reporter

The `/etc/reporterd.ini` file is used to control various aspects of the reporter daemon behavior. Once the configuration file is modified, the new settings take effect in one minute. You do not need to restart the service. `reporterd.ini` is an `.ini`-style configuration file.

Table 6-1, Table 6-2, and Table 6-3 describe the three sections in the `/etc/reporterd.ini` file.

Table 6-1 Reports

Command	Description
`ReportServerURL`	Set the reporting server URL. The format is http://serverip:port/Reporting. The reporting server uses port 8014 by default. You must set the reporting server IP address and port number to enable the service to upload log records and inventory information.
`FileSizeLimit`	Configure the size, in megabytes, of the temporary files that are uploaded to the reporting server. The default is 2 MB.
`MinDiskSize`	Configure the amount of available disk space on the current file system, in megabytes, that triggers the reporterd service to stop processing files. The default is 100 MB.
`RunNowPeriod`	Specify the duration of Run Now mode in minutes. The default is five minutes.
`ServerGroup`	Specify the server group name. The default is Symantec AntiVirus for Linux.
`Encoding`	Specify which character encoding to use for the reporterd service. The default blank value means to use the current operating system character encoding as the default character encoding. Note: You should typically leave this parameter value blank unless you want to override the default.

Table 6-2 Inventory

Command	Description
`DeleteLogDays`	Specify how old, in days, log files should be before they are deleted. The default is seven days.

Table 6-2 Inventory *(continued)*

Command	Description
`Frequency`	Specify how often, in minutes, to send log records to the reporting server. The default is 1440 minutes.
`Debug`	Specify whether to generate debug information in the log file. The default is OFF(0); a value of 1 is ON.

Table 6-3 LogSender

Command	Description
`AggregatonPeriod`	Specify how long, in minutes, the Log Sender Agent waits before aggregating redundant virus events. The default is five minutes.
`DeleteLogDays`	Specify how old, in days, log files should be before they are deleted. The default is seven days. Specify how old, in days, log files should be before they are deleted. The default is seven days.
`Frequency`	Specify how often, in minutes, to send log records to the reporting server. The default is five minutes.
`Debug`	Specify whether to generate debug information in the log file. The default is OFF(0); a value of 1 is ON.

Man pages for the Symantec AntiVirus for Linux Reporter

The Symantec AntiVirus for Linux Reporter provides two manual pages, one for the reporter daemon (service), and one for the reporter configuration file.

- To get help information for `reporterd`, type:

  ```
  # man 8 reporterd
  ```

- To get help information for reporterd.ini, type:

  ```
  # man 5 reporterd.ini
  ```

Known issues for the Symantec AntiVirus for Linux Reporter

The Symantec AntiVirus for Linux Reporter has the following issues in the Symantec Endpoint Protection Manager console:

- Filenames that include some special characters ('?', '"', '\n') do not appear correctly.
- In the Symantec Endpoint Protection Manager logs, the operating system for the Linux client across platforms appears as unsupported, unknown, or blank.

  The Reporter uses the Symantec Endpoint Protection Manager legacy reporting channel, which cannot upload operating system-related information in the console interface. To work around this issue, you configure the Server Group in the Reporter. You then filter Linux clients from Windows or Mac clients in the Symantec Endpoint Protection Manager console by using the domain name.

To configure the Server Group

1. Open the `/etc/reporterd.ini` configuration file on the SAVFL Reporter client.
2. In the **Reporting** section of the `reporterd.ini` file, change the **ServerGroup** parameter to the desired group.

   By default, this parameter is set to **Symantec AntiVirus for Linux**.
3. In the Symantec Endpoint Protection Manager console, select the type of log to view and then click **Advanced Settings**.
4. Enter the **Domain** filter setting, click **Save Filter**, enter a name, and then click **OK**.
5. Click **View Log** using this filter to see the specified **ServerGroup** clients' log data.

Appendix A

Troubleshooting and error messages

This appendix includes the following topics:

- Symantec AntiVirus for Linux installation by GUI rpm manager may display a warning message
- Auto-Protect is not supported for use on SUSE Linux Enterprise Server 11 (x86_64) with the kernel version 2.6.27.19-5
- Error messages may appear after you install the SAVUI installation package
- English date format appears in the user interface if the Yet another Setup Tool (YaST) installation program is used to install Symantec AntiVirus for Linux on computers that run non-English language operating systems
- You must install the i686-based dependent packages on 64-bit computers that run Fedora, RedHat ES 6.x Linux or Oracle Linux before you install Symantec AntiVirus for Linux
- Unity Panel Icon missing in Ubuntu 11.x (and later) desktop
- rpm -U does not work for upgrading the savjlu package

Summary of material from MR1 to MR14

The following material applies to the current release, and has been gathered from changes made in previous releases

Files in the `/etc/symantec` directory are not removed when you uninstall Symantec AntiVirus

The `VPREGDB.BAK`, `VPREGDB.DAT`, and `VPREGDB.SAV` configuration files are deliberately retained in the `/etc/symantec` directory after you use rpm to uninstall Symantec AntiVirus. These files may be used to save and restore Symantec AntiVirus configuration data. To reinstall Symantec AntiVirus with its default configuration, delete these existing `VPREGDB.BAK`, `VPREGDB.DAT`, and `VPREGDB.SAV` files before you reinstall.

Default logging level of daemons has been changed from `debug` to `info`

The default logging level of the daemons has been changed from `debug` to `info` to enhance performance. To change the logging levels, refer to the man page, `rtvscand(8)`.

Gjc interferes with Java LiveUpdate

By default some Linux distributions, such as Ubuntu, install with the GNU Java(tm), which has problems running Java LiveUpdate.

To use Java LiveUpdate services, make sure Sun JRE 1.4.2 or later is installed instead of GNU Java.

Java Cryptography Extensions

Ensure Unlimited Strength Java Cryptography Extension (JCE) policy files are used rather than limited jar policy files.

HTTP port 80 should be opened for Java LiveUpdate (e.g., ESX3.5)

Some Linux systems install firewalls by default. If the firewall blocks HTTP port 80, it denies accesses to the default Symantec LiveUpdate servers . Make sure that HTTP port 80 is open. For example, on ESX 3.5, type the following command:

```
#esxcfg-firewall --openPort 80,tcp,out,http80
```

If you use proxy servers, please configure them accordingly.

New SAV command line options

The following are new command line options:

- `sav scheduledscan -p|--stop scan_id` stops a scheduled scan that is in progress.
- `sav manualscan -c|--clscan [pathname|-]` initiates a synchronous manual scan that does not return control to the command prompt until the scan is complete.
- `sav quarantine -d|--delete/-r|--restore/-p|--repair/-i|--info "*"` deletes, restores, repairs, or provides detailed information about all of the quarantined items, respectively.

For more information about the command instructions, please refer to the man page. Note that these options also appear in the guide.

Registry key root change

The new registry root key has been changed from `\VirusProtect6` to `\Symantec Endpoint Protection\AV`. Use this new value when you follow the examples in the documentation. This version of the documentation has been corrected, but if you see a reference to `\VirusProtect6`, it is there because of a documentation error, and should be read as `\Symantec Endpoint Protection\AV`.

Customized installation path support for rpm packages

The user can install rpm packages to a customized installation path with the option prefix, but you must install these rpm packages to the same path. For example, you can type the following command **`rpm -Uhv --prefix`** ***`yourpath`*** **`*.rpm`**.

Debian and Ubuntu users should use `sudo`

To install and run Symantec AntiVirus for Linux commands, Debian and Ubuntu users should use `sudo`. Do not use `su` to root for these actions. In addition, ensure that the user who is running the command is in the `sudoers` list.

Xen kernel details

Symantec AntiVirus for Linux supports -xen kernels of a paravirtulized guest operating system. It does not need any specific configurations to install or load Auto-Protect modules. The product does not support other variant kernels, such as -xenU.

You must install the i686-based dependent packages on the 64-bit computers that run Debian or Ubuntu Linux before you install SAV for Linux

Since many of the executable files in SAV packages are 32-bit programs, you must install the i686-based dependent packages on the 64-bit computers that run Debian or Ubuntu Linux before you install the SAV for Linux packages. If the i686-based dependent packages are not already on the computer, you can install them by typing the following command:

```
sudo apt-get install ia32-libs
```

Auto Protect is not enabled on remote disk partitions by default

By default, Auto Protect will not capture file access on remote disk partitions, such as NFS. To enable this feature, please set the following registry key`\HKEY_LOCAL_MACHINE\Symantec Endpoint Protection\AV\Storages\FileSystem\RealTimeScan\Networks` to `1`.

The Auto-Protect kernel modules source has been partially opened

Based on requests from customers, Symantec partially opens the Auto-Protect kernel modules source code. Symantec provides the relevant library files so that customers can compile the Auto-Protect kernel modules themselves. For more information, refer to `README` file in the source tar-ball.

Symantec AntiVirus for Linux Implementation Guide -- change in LiveUpdate behavior

In the section titled "About the Java LiveUpdate configuration file," the definition of the working directory in the first row of the table was out of date. The local package directory is no longer removed under any circumstances when Java LiveUpdate exits.

Note: This is a change from previous behavior, and that sentence has been changed in this release.

Symantec AntiVirus for Linux installation by GUI rpm manager may display a warning message

If you install Symantec AntiVirus for Linux by using the GUI rpm manager without using the command line, you may see a warning message that states that the installer is not a known application. You may safely ignore this message. Click **Ignore**, and the installation should succeed without problems.

Auto-Protect is not supported for use on SUSE Linux Enterprise Server 11 (x86_64) with the kernel version 2.6.27.19-5

Loading the Auto-Protect kernel module (symev) on SUSE Linux Enterprise Server 11 (x86_64) with the kernel version 2.6.27.19-5 causes the operating system to stop responding due to an operating system defect. If you want to use the Auto-Protect feature on SUSE Linux Enterprise Server 11 (x86_64), you must upgrade your kernel to version 2.6.27.21-0.1.2 or later. For more information, refer to bug 439348 in the Novell Bugzilla.

Error messages may appear after you install the SAVUI installation package

After you install the SAVUI installation package on some platforms, you may see the following error messages in the savui-install.log file:

- `* QSettings:sync: filename is null/empty`
- `* QDate::setYMD: Invalid date 0000-00-00`

After the first restart, you may see the following strings in the savui-install.log file:

- `* ICE default IO error handler doing an exit(), pid = 3566, errno = 0`
- `* savtray: Fatal IO error: client killed`

You can ignore these strings. They do not reappear.

English date format appears in the user interface if the Yet another Setup Tool (YaST) installation program is used to install Symantec AntiVirus for Linux on computers that run non-English language operating systems

If you use YaST to install the savui package on non-English language versions of SUSE Linux, the savtray user interface date format appears as MM/DD/YY instead of YY/MM/DD. To get the correct date format to appear, you can restart the savtray program. Other installation methods do not have this issue.

You must install the i686-based dependent packages on 64-bit computers that run Fedora, RedHat ES 6.x Linux or Oracle Linux before you install Symantec AntiVirus for Linux

Since many of the executable files in SAV packages are 32-bit programs, you must install the i686-based dependent packages on the 64-bit computers that run Fedora Linux before you install the SAV Linux packages. If the i686-based dependent packages are not already on the computer, you can install them by using the following command:

```
yum install glibc.i686 libgcc.i686 libX11.i686
```

Unity Panel Icon missing in Ubuntu 11.x (and later) desktop

In 11.x Ubuntu, after the savui deb package installs, if the tray icon is missing on the Unity panel, run the following command lines on a desktop terminal. Use the user account you logged in with.

-
  ```
  #systraywhitelist=`gsettings get com.canonical.Unity.Panel
  systray-whitelist
  ```

-
  ```
  #echo $systraywhitelist
  ```

If the output includes the `Savtray` string, then log on to the desktop system again. If not, execute the command line:

-
  ```
  #systraywhitelist=`echo $systraywhitelist | sed "s/, 'Savtray'//g"`
  ```

-
  ```
  #systraywhitelist="${systraywhitelist%]}, 'Savtray']"
  ```

-
  ```
  #gsettings set com.canonical.Unity.Panel systray-whitelist
  "$systraywhitelist"
  ```

Log on to the desktop system again.

`rpm -U` does not work for upgrading the savjlu package

This `rpm -U` command does not work for upgrading. To upgrade LiveUpdate, uninstall old versions and then install the new version by typing:

- **`rpm -e`**
- **`rpm -i`**

Index