Symantec™ Endpoint Protection 14.x for Linux Client Guide

Contents

Chapter 1

Protecting Linux computers with Symantec Endpoint Protection

This chapter includes the following topics:

About Symantec Endpoint Protection for Linux

The Symantec Endpoint Protection client combines different types of scans to secure your computers against virus and spyware attacks.

Auto-Protect continuously inspects all computer files for viruses and security risks as they are accessed on the client computer. Scheduled scans and manual scans periodically scan your entire computer for viruses and security risks.

By default, Symantec Endpoint Protection automatically attempts to repair any virus that it finds. If it can't repair the file, the client safely quarantines the file so that it cannot harm your computers.

The Symantec Endpoint Protection Manager administrator configures the specific actions that the client should take on the computer to repair infected files. If your administrator gives you permission, you can also configure these actions using the command line.

See "What happens when a virus is detected" on page 7.

Symantec Endpoint Protection client for Linux system requirements

This section includes the system requirements for version 14.2.

For the system requirements for earlier versions of Symantec Endpoint Protection, or for the most current version of these system requirements, see the following webpage:

Release notes, new fixes, and system requirements for all versions of Endpoint Protection

Table 1-1 Symantec Endpoint Protection client for Linux system requirements

Component	Requirements
Hardware	■ Intel Pentium 4 (2 GHz) or later processor ■ 1 GB of RAM ■ 7 GB of available hard disk space
Operating systems	■ Amazon Linux ■ CentOS 6U3 - 6U9, 7 - 7U4; 32-bit and 64-bit ■ Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit ■ Fedora 16, 17; 32-bit and 64-bit ■ Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8; 7, 7U1, 7U2, 7U3 ■ Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U4 ■ SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12, 12 SP1 - 12 SP3, 64-bit ■ SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12 SP3, 64-bit ■ Ubuntu 12.04, 14.04, 16.04; 32-bit and 64-bit For a list of supported operating system kernels, see Supported Linux kernels for Symantec Endpoint Protection.
Graphical desktop environments	You can use the following graphical desktop environments to view the Symantec Endpoint Protection for Linux client: ■ KDE ■ Gnome ■ Unity

Table 1-1 Symantec Endpoint Protection client for Linux system requirements *(continued)*

Component	Requirements
Other environmental requirements	■ Glibc Any operating system that runs glibc earlier than 2.6 is not supported. ■ i686-based dependent packages on 64-bit computers Many of the executable files in the Linux client are 32-bit programs. For 64-bit computers, you must install the i686-based dependent packages before you install the Linux client. If you have not already installed the i686-based dependent packages, you can install them by command line. This installation requires superuser privileges, which the following commands demonstrate with `sudo`: ■ For Red Hat-based distributions: `sudo yum install glibc.i686 libgcc.i686 libX11.i686` ■ For Debian-based distributions: `sudo apt-get install ia32-libs` ■ For Ubuntu-based distributions: `sudo apt-get install libx11-6:i386 libgcc1:i386 libc6:i386` ■ net-tools or iproute2 Symantec Endpoint Protection uses one of these two tools, depending on what is already installed on the computer. ■ XFS file systems that contain inode64 attributes are not supported. ■ Developer tools Auto-compile and the manual compile process for the Auto-Protect kernel module require that you install certain developer tools. These developer tools include gcc and the kernel source and header files. For details on what to install and how to install them for specific Linux versions, see: Manually compile Auto-Protect kernel modules for Endpoint Protection for Linux

Getting started on the Linux client

The Symantec Endpoint Protection Manager administrator may have enabled you to configure the settings on the Linux client.

Table 1-2 Steps to get started on the Linux client

Step	Action
Step 1: Install the Linux client.	The Symantec Endpoint Protection Manager administrator provides you with the installation package for a managed client or sends you a link by email to download it. You can also uninstall an unmanaged client, which does not communicate with Symantec Endpoint Protection Manager in any way. The primary computer user must administer the client computer, update the software, and update the definitions. You can convert an unmanaged client to a managed client. See "Importing client-server communication settings into the Linux client" on page 8.
Step 2: Check that the Linux client communicates with Symantec Endpoint Protection Manager.	Double-click the Symantec Endpoint Protection shield. If the client successfully communicates with Symantec Endpoint Protection Manager, then server information displays under **Management**, next to **Server**. If you see **Offline**, then contact the Symantec Endpoint Protection Manager administrator. If you see **Self-managed**, then the client is unmanaged. The shield icon also indicates both the management and the communication status. See "About the Linux client graphical user interface" on page 7.
Step 3: Verify Auto-Protect is running.	Double-click the Symantec Endpoint Protection shield. Auto-Protect's status displays under **Status**, next to **Auto-Protect**. You can also check the status of Auto-Protect through the command-line interface: `sav info -a` See sav on page 15.
Step 4: Check that the definitions are up to date.	LiveUpdate automatically launches after installation is complete. You can verify that definitions are updated when you double-click the Symantec Endpoint Protection shield. The date of the definitions displays under **Definitions**. By default, LiveUpdate for the Linux client runs every four hours. If the definitions appear outdated, you can click **LiveUpdate** to run LiveUpdate manually. You can also use the command-line interface to run LiveUpdate: `sav liveupdate -u` See sav on page 15.
Step 5: Run a scan.	By default, the managed Linux client scans all files and folders daily at 12:30 A.M. However, you can launch a manual scan using the command-line interface: `sav manualscan -s` *`pathname`* **Note:** The command to launch a manual scan requires superuser privileges. See sav on page 15.

Symantec Endpoint Protection for Linux Frequently Asked Questions (SEP for Linux FAQ)

About the Linux client graphical user interface

If your Linux computer includes a graphical user interface (GUI), the Symantec Endpoint Protection for Linux client displays a yellow shield notification area icon on the status tray. The icon provides information about whether the client is connected to a management server and the protection status.

You perform most management tasks using the command-line interface. However, you can use the Symantec Endpoint Protection client GUI to perform the following tasks:

- Review information about the version of the product and the virus definitions.
- Check the status of the client's protection, which includes whether Auto-Protect is enabled, and the status of any scheduled scans or manual scans.
- Run LiveUpdate to get the latest virus definitions and product updates.
- Get information about whether the client is unmanaged, or is managed and connects to Symantec Endpoint Protection Manager to receive updated policies.

You can also perform these tasks from the command line.

Table 1-3 Symantec Endpoint Protection for Linux client status icons

Icon	Description
	The client is unmanaged and functions correctly. The icon is a plain yellow shield.
	The client is managed, functions correctly, and successfully communicates with Symantec Endpoint Protection Manager. The icon is a yellow shield with a green dot.
	The client is managed, functions correctly, and does not successfully communicate with Symantec Endpoint Protection Manager. The icon is a yellow shield with a light yellow dot that contains a black exclamation mark.
	The client fails to function correctly because of disabled components, such as Auto-Protect, the real-time scanning service (rtvscand), or the client management service (smcd). The icon is a yellow shield with a white dot outlined in red and a red slash across the dot.

See "Getting started on the Linux client" on page 5.

What happens when a virus is detected

If a scan detects a virus, Symantec Endpoint Protection attempts to clean the virus from the infected file and repair the effects of the virus by default. If the file is cleaned, the virus is

successfully and completely removed. If Symantec Endpoint Protection cannot clean the file, Symantec Endpoint Protection attempts a second action, quarantining the infected file so that the virus cannot spread. For a managed client, the Symantec Endpoint Protection Manager administrator can also configure Symantec Endpoint Protection to delete infected files.

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

Typically, you do not need to take any action when a virus is detected. The Symantec Endpoint Protection Manager administrator configures Symantec Endpoint Protection to take appropriate action.

See "About Symantec Endpoint Protection for Linux" on page 3.

Importing client-server communication settings into the Linux client

After you install an unmanaged Symantec Endpoint Protection for Linux client, you can convert it to a managed client to centrally manage the client's policies and status with Symantec Endpoint Protection Manager. A managed client communicates with and reports its status and other information to Symantec Endpoint Protection Manager.

You can also use this procedure to reconnect a previously orphaned client with Symantec Endpoint Protection Manager.

Note: You must have superuser privileges to perform this procedure. The procedure uses `sudo` to demonstrate this elevation of privilege as required.

The text *path-to-sav* represents the path to the sav command. The default path is /opt/Symantec/symantec_antivirus/.

To import the client-server communication settings file into the Linux client

1. You or the Symantec Endpoint Protection Manager administrator must first export the communication settings file from Symantec Endpoint Protection Manager and copy it to the Linux computer. Ensure that the file name is `sylink.xml`.

2 On the Linux computer, open a terminal window and enter the following command:

```
sudo path-to-sav/sav manage -i path-to-sylink/sylink.xml
```

Where *path-to-sylink* represents the path to which you copied `sylink.xml`.

For example, if you copied it to your user profile's desktop, enter:

```
sudo path-to-sav/sav manage -i ~/Desktop/sylink.xml
```

3 A successful import returns OK. To further verify the managed status, enter the following command, which displays the policy serial number for a successful import:

```
path-to-sav/sav manage -p
```

Uninstalling the Symantec Endpoint Protection client for Linux

You uninstall the Symantec Endpoint Protection client for Linux with the script that the installation provides.

Note: You must have superuser privileges to uninstall the Symantec Endpoint Protection client on the Linux computer. The procedure uses `sudo` to demonstrate this elevation of privilege.

To uninstall the Symantec Endpoint Protection client for Linux

1 On the Linux computer, open a terminal application window.

2 Navigate to the Symantec Endpoint Protection installation folder with the following command:

```
cd /opt/Symantec/symantec_antivirus
```

The path is the default installation path.

3 Use the built-in script to uninstall Symantec Endpoint Protection with the following command:

```
sudo ./uninstall.sh
```

Enter your password if prompted.

This script initiates the uninstallation of the Symantec Endpoint Protection components.

4 At the prompt, type **Y** and then press **Enter**.

Uninstallation completes when the command prompt returns.

Note: On some operating systems, if the only contents of the `/opt` folder are the Symantec Endpoint Protection client files, the uninstaller script also deletes `/opt`. To recreate this folder, enter the following command: **`sudo mkdir /opt`**

To uninstall using a package manager or software manager, see the documentation specific to your Linux distribution.

Appendix A

Symantec Endpoint Protection client for Linux command line reference

This appendix includes the following topics:

rtvscand

`rtvscand` – The command-line interface to manage rtvscan, which is the Symantec Endpoint Protection service that protects Linux client computers from viruses and other security risks.

SYNOPSIS

`rtvscand [-Fchwx] [-f log_facility] [-k shutdown | check] [-l log_severity] [-p pid_file] [-r report_file] [-s path]`

DESCRIPTION

`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 defaults should be required.

You must have superuser privileges to use rtvscand.

By default, rtvscand is located in /opt/Symantec/symantec_antivirus.

OPTIONS

`rtvscand -F`

Run the service in the foreground. This option prevents the service from running as a daemon.

`rtvscand -c`

Write log entries also to the console (stderr).

`rtvscand -h`

Print help information to the standard output.

`rtvscand -w`

Wait for the debugger to be attached to the process.

`rtvscand -x`

Enable debug mode. Debug mode provides verbose logs and runtime checks.

`rtvscand -f log_facility`

Specify the log facility to use when logging to syslog. Possible values are **daemon**, **user**, and **local0** through **local7**. The default is **daemon**.

You must also configure the `/etc/syslog.conf` file to specify handling for the facility.

`rtvscand -k check`

Send a signal to the running copy of rtvscand to determine if rtvscand is currently running, print out a message, and exit. The running copy is identified by a process with the pid that

matches the pid stored in the pid file. If there is a running copy, the command returns a 0. If there is no running copy, the command returns a 1.

When specifying the -k option and using a non-default pid file, the -p option 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.

`rtvscand -k shutdown`

Send a signal to the running copy of rtvscand to shut down, and then exit. The running copy is identified by a process with the pid that matches the pid stored in the pid file. The process attempts to perform a graceful shutdown.

When specifying the -k option and using a non-default pid file, the -p option 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.

`rtvscand -l` *`log_severity`*

Log all messages up to and including the specified severity level. The severity level must be one of the following: **none**, **emerg**, **alert**, **crit**, **error**, **warning**, **notice**, **info**, **debug**.

`rtvscand -p` *`pid_file`*

Specify to use the given pid file instead of the default `/var/run/symantec/rtvscand.pid`. 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.

`rtvscand -r` *`report_file`*

Specifies the use of a given report file instead of the default `/var/log/symantec/rtvscand_report.log`. You should always use absolute path names when configuring rtvscand.

`rtvscand -s` *`path`*

Set the working directory that the service runs in. You should always use absolute path names when configuring rtvscand.

This typically does not need to be changed from the default, which is the root directory (/).

FILES

`/etc/sysconfig/rtvscand`

This configuration file specifies command-line options that are passed to the rtvscand program when it is started with the init.d script. To use this file, you must set the options to rtvscand between the quotes as shown 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.

sav

`sav` – The command-line interface to manage Symantec Endpoint Protection.

SYNOPSIS

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

sav [-h|--help]

sav autoprotect [-e|--enable] | [-d|--disable]

sav manualscan [-t|--stop] | [-s |--scan [pathname|-]] | [-c|--clscan
[pathname|-]]

sav scheduledscan [-l|--list] | [-n|--info scan_id] | [-p|--stop scan_id] |
[-d|--delete scan_id] | [-e|--enable scan_id | [-s|--disable scan_id] |
[-c|--create scan_id [-f|--frequency [daily|weekly|monthly]] [-i|--interval
[HH:MM|DDD|D]] [-t|--time [HH:MM]] [-m|--missedevents [0|1]] pathname|-]

sav liveupdate [-u|--update] | [-v|--view] | [-s|--schedule [-f|--frequency
[continuously|hourly|daily|weekly]] [-i|--interval [HH|HH:MM|DDD]] [-t|--time
[HH:MM]] [-r|--retrywindow [HH|DD|MM]] [-d|--randomizewindow [DD|HH]]]

sav quarantine [-l|--list] | [-d|--delete id] | [-r|--restore id] | [-p|--repair
id] | [-i|--info id]

sav definitions [-r|--rollback]

sav info [-d|--defs] | [-e|--engine] | [-p|--product] | [-s|--scanner] |
[-a|--autoprotect] | [-t|--threats]

sav manage [-g|--group] | [-h|--heartbeat] | [-i|--import pathname] |
[-o|--location] | [-p|--profile] | [-s|--server] | [-t|--time] | [-l|--license]

sav log [-e|--export [-f|--from start_id] [-t|--to end_id] pathname]
```

DESCRIPTION

Symantec Endpoint Protection for Linux provides a command-line interface to perform the following tasks:

- Enable and disable Auto-Protect
- Start and stop manual scans
- Create, delete, enable, and disable scheduled scans
- Manage LiveUpdate sessions

- Manage Virus and Spyware Protection
- Manage the local Quarantine
- Display information about protection on the client computer
- Manage client communication with Symantec Endpoint Protection Manager
- Export logs from the client computer

All command output can be parsed by third-party tools. Header information is not provided for the columns in the output.

Most `sav` commands require one or more parameters.

You must have superuser privileges to use all `sav` commands except the following:

- `sav liveupdate -u`
- `sav info [-a] [-d] [-e] [-p]`
- `sav manage [-g] [-h] [-o] [-p] [-s] [-t] [-l]`

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

OPTIONS

`sav -q|--quiet` *`command parameter(s)`*

Displays only the requested information; suppresses other information such as status and error messages. This option can be used with any other command and its parameters.

`sav -h|--help`

Displays help information.

`sav autoprotect -e|--enable`

Enables Auto-Protect.

`sav autoprotect -d|--disable`

Disables Auto-Protect.

`sav manualscan [-s|--scan [`*`pathname`*`|-]]`

Starts a manual scan.

pathname specifies the file and directory list to scan. To specify this list, type a list of files and directories separated by line feeds and ending with an end of file signal, such as CTRL-D. If a directory is specified, all subdirectories are also scanned. Wildcard characters are supported.

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 of `VirusProtect6MaxInput` to increase this limit. To remove the limit entirely, set the value of `VirusProtect6MaxInput` to 0. See also `symcfg`.

If you specify a hyphen (-) instead of a list of files and directories, then the list of path names is read from the standard input. You can use commands that produce a list of files or path names separated by line feeds.

Submitting a very long list of items to this command can negatively affect performance. Symantec recommends that you limit lists to a maximum of a few thousand items.

`sav manualscan [-c|--clscan [pathname|-]]`

Starts a manual scan that does not return control to the command prompt until the scan is complete. The settings for this option are otherwise identical to the settings for the -s option.

`sav manualscan -t|--stop`

Stops a manual scan that is in progress.

`sav scheduledscan -l|--list`

Lists administrator-defined scheduled scans and local scheduled scans with their current status, which is either enabled or disabled.

`sav scheduledscan -n|--info scan_id`

Displays detailed information about the scan specified by *scan_id*.

`sav scheduledscan -d|--delete scan_id`

Deletes the local scheduled scan specified by *scan_id*. Administrator-defined scheduled scans cannot be deleted manually.

`sav scheduledscan -e|--enable scan_id`

Enables the local scheduled scan specified by *scan_id*. Administrator-defined scheduled scans cannot be enabled manually.

`sav scheduledscan -s|--disable scan_id`

Disables the local scheduled scan specified by *scan_id*. Administrator-defined scheduled scans cannot be disabled manually.

`sav scheduledscan -p|--stop scan_id`

Stops the local scheduled scan specified by *scan_id* that is in progress. Administrator-defined scheduled scans cannot be stopped manually.

`sav scheduledscan -c|--create scan_id parameters pathname|-`

Creates a new local scheduled scan that is identified by *scan_id*, which must be unique.

pathname specifies the file and directory list to scan. To specify this list, type a list of files and directories separated by line feeds and ending with an end of file signal, such as CTRL-D. If a directory is specified, all subdirectories are also scanned. Wildcard characters are supported.

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 of `VirusProtect6MaxInput` to increase this limit. To remove the limit entirely, set the value of `VirusProtect6MaxInput` to 0. See also `symcfg`.

If you specify a hyphen instead of a list of files and directories, then the list of path names is read from the standard input. You can use commands that produce a list of files or path names separated by line feeds.

Submitting a very long list of items to this command can negatively affect performance. Symantec recommends that you limit lists to a maximum of a few thousand items.

Use the following additional parameters to specify the details of a scheduled scan:

`-f|--frequency [daily|weekly|monthly]`

Required. Specifies the scan frequency.

`-i|--interval [HH:MM|DDD|D]`

Specifies the interval between scans. Depends on `frequency`.

If `frequency` is `daily`, the interval must be `HH:MM`, where HH = the hour (00 - 23) and MM = the minute (00-59).

If `frequency` is `weekly`, the interval must be `DDD`, where DDD = one of **Sun, Mon, Tue, Wed, Thu, Fri, Sat**.

If `frequency` is `monthly`, the interval must be `D`, where D = any value from 1 to 31.

`-t|--time [HH:MM]`

HH = the hour (00 - 23) and MM = the minute (00 - 59). Not used for daily frequency.

`-m|--missedevents`

Enables or disables missed event processing. The default is 0 (disabled).

0 = disabled

1 = enabled

`sav liveupdate -u|--update`

Runs LiveUpdate immediately.

`sav liveupdate -v|--view`

Displays the current LiveUpdate schedule.

`sav liveupdate -s|--schedule [`*`parameters`*`]`

Creates a new schedule for Automatic LiveUpdate sessions. The following parameters are used to set the schedule:

`-f|--frequency [continuously|hourly|daily|weekly]`

Required. Specifies the update frequency.

`-i|--interval [HH|HH:MM|DDD]`

Specifies the interval between LiveUpdate sessions. Depends on `frequency`.

If `frequency` is `continuously` , the interval is 15 minutes.

If `frequency` is `hourly`, the interval must be `HH`, where HH = the hour (00 - 23).

If `frequency` is `daily`, the interval must be `HH:MM`, where HH = the hour (00 - 23) and MM = the minute (00-59).

If `frequency` is `weekly`, the interval must be `DDD`, where DDD = one of **Sun, Mon, Tue, Wed, Thu, Fri, Sat**.

`-t|--time [HH:MM]`

Specifies HH = the hour (00 - 23) and MM = the minute (00 - 59). Used for weekly frequency only.

`-r|--retrywindow [HH|DD|MM]`

Specifies the amount of time during which the client computer tries to run LiveUpdate if the scheduled LiveUpdate session fails. If the `frequency` is `hourly`, the `retrywindow` is in hours (HH). If the `frequency` is `daily`, the `retrywindow` is in days (DD). If the `frequency` is `weekly`, the `retrywindow` is in months (MM). Does not apply to `continuously`.

`-d|--randomizewindow [DD|HH]]`

Specifies a randomization option. You can stagger LiveUpdate sessions, plus or minus the value that is specified, to minimize the effect on network traffic. If `frequency` is daily, the `randomizewindow` value specifies the number of hours around which to randomize sessions. If `frequency` is weekly, the `randomizewindow` value specifies the number of days around which to randomize sessions. This argument is not supported for the `continuously` or `hourly` frequencies.

`sav quarantine -l|--list`

Lists all the items that are in the local Quarantine.

`sav quarantine -d|--delete` *`id`*

Deletes the specified item from the Quarantine. To view the *id* of an item, list the items that are in the Quarantine. `--delete`, `--restore`, `--repair`, and `--info` accept a regular expression in place of *id*. When using a regular expression, make sure that special characters are properly escaped. For example, use `sav quarantine -d "*"`, not `sav quarantine -d *`.

`sav quarantine -r|--restore` *`id`*

Restores the quarantined item that is specified. To view the *id* of an item, list the items that are in the Quarantine.

`sav quarantine -p|--repair` *`id`*

Attempts to repair the quarantined item that is specified. To view the *id* of an item, list the items that are in the Quarantine.

`sav quarantine -i|--info id`

Provides detailed information about the quarantined item that is specified. To view the *id* of an item, list the items that are in the Quarantine.

`sav definitions -r|--rollback`

Rolls back the definitions in use to the last known good version.

`sav info -a|--autoprotect`

Displays the status of Auto-Protect on the computer.

`sav info -d|--defs`

Displays the version and date of the current virus and security risk definitions in use on the computer.

`sav info -e|--engine`

Displays the version of the scan engine in use on the computer.

`sav info -p|--product`

Displays the product version in use on the computer.

`sav info -s|--scanner`

Displays whether a scan is in progress on the computer.

`sav info -t|--threats`

Displays the list of threats and security risks that the computer is currently protected against. You must have superuser privileges to display this information.

`sav manage -g|--group`

Displays the management server group that the client belongs to.

`sav manage -h|--heartbeat`

Triggers a heartbeat immediately. Then the managed client can download the profile and upload the status without any wait.

`sav manage -i|--import pathname`

Downloads a client communication file from the management server to the client. The *pathname* can be full path name or relative path name.

`sav manage -o|--location`

Displays the location that is defined for the client by the management server.

`sav manage -p|--profile`

Displays the current profile series number for the managed client.

`sav manage -s|--server`

Displays the IP address of the management server that the client is currently connected to.

`sav manage -t|--time`

Displays most recent time when the client connected to the management server.

`sav manage -l|--license`

Displays the client license status.

`sav log -e|--export` *`parameters`*

Exports the system logs to specified file or console. The following parameters are used to set the details of the log export:

`-f|--from` *`start_id`*

start_id specifies the index number of the first log to export. If *start_id* is not specified, the export defaults to the first log.

`-t|--to` *`end_id`*

end_id specifies the index number of the last log to export. If *end_id* is not specified, the export defaults to the last log.

`pathname`

Specifies the full pathname of the file that the logs are exported to. If *pathname* is not specified, the export defaults to the console.

savtray

`savtray` – The command-line interface to the graphical user interface for Symantec Endpoint Protection for Linux.

SYNOPSIS

`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]`

DESCRIPTION

`savtray` provides a simple graphical interface to Symantec Endpoint Protection for Linux. It lets users review information about their security status, receive notifications about risk events, and start LiveUpdate sessions.

By default, savtray is located in /opt/Symantec/symantec_antivirus.

OPTIONS

`savtray -bg|-background` *`color`*

Sets the default background color and an application palette. Light and dark shades are calculated.

`savtray -btn|-button` *`color`*

Sets the default button color.

`savtray -cmap`

Causes the application to install a private color map on an 8-bit display.

`savtray -display` *`display`*

Species the name of the X server to use. The default is $DISPLAY.

`savtray -fg|-foreground` *`color`*

Sets the default foreground color that is used for text and graphics.

`savtray -fn|-font` *`font`*

Defines the application font. The font should be specified using an X logical font description.

`savtray -geometry` *`geometry`*

Specifies the initial size and location of the window.

`savtray -name` *`name`*

Sets the application name.

`savtray -ncols count`

Limits the number of colors that are allocated on an 8-bit display.

`savtray -reverse`

Causes text to be formatted for right-to-left languages rather than for left-to-right

`savtray -session=session|-session session`

Restores the application from an earlier session.

`savtray -style=style|-style style`

Sets the application GUI style. Possible values are motif, windows, and platinum.

`savtray -title title`

Sets the application caption.

`savtray -visual TrueColor`

Forces the application to use a TrueColor visual on an 8-bit display.

`savtray -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.

smcd

`smcd` – The Symantec management client service, which runs as a daemon process.

SYNOPSIS

```
smcd [-Fchwx] [-f log_facility] [-k shutdown | report | check] [-l log_severity]
[-p pid_file] [-r report_file] [-s path]
```

DESCRIPTION

The smcd service runs as a daemon process and provides clients with communication to a Symantec Endpoint Protection management server. This service is typically started automatically by the system initialization scripts. No changes to the defaults should be required.

You must have superuser privileges to use smcd.

By default, smcd is located in /opt/Symantec/symantec_antivirus.

OPTIONS

`smcd -F`

Run the service in the foreground. This option prevents the service from running as a daemon.

`smcd -c`

Write log entries also to the console (stderr).

`smcd -h`

Print help information to the standard output.

`smcd -w`

Wait for the debugger to be attached to the process.

`smcd -x`

Enable debug mode. Debug mode provides verbose logs and runtime checks.

`smcd -f log_facility`

Specify the log facility to use when logging to syslog. Possible values are **daemon**, **user**, and **local0** through **local7**. The default is **daemon**.

To set this up, you must also configure your `/etc/syslog.conf` file to specify handling for the facility.

`smcd -k shutdown`

Send a signal to the running copy of smcd to shut down and then exit. The running copy is identified by a process with the pid that matches the pid stored in the pid file. The process attempts to perform a graceful shutdown.

When specifying the -k option and using a non-default pid file, the -p option must also be given to ensure that the signal is sent to the correct smcd instance, even if there is only a single smcd instance running.

`smcd -k report`

Send a signal to the running copy of smcd to report its status into a log file. The default log file is `/var/log/symantec/smcd_report.log`, but you can configure the log location with the -r option.

When specifying the -k option and using a non-default pid file, the -p option must also be given to ensure that the signal is sent to the correct smcd instance, even if there is only a single smcd instance running.

`smcd -k check`

Send a signal to the running copy of smcd to determine if smcd is currently running, print out a message, and exit. The running copy is identified by a process with the pid that matches the pid stored in the pid file. If there is a running copy, the command returns a 0. If there is no running copy, the command returns a 1.

When specifying the -k option and using a non-default pid file, the -p option must also be given to ensure that the signal is sent to the correct smcd instance, even if there is only a single smcd instance running.

`smcd -l` *`log_severity`*

Log all messages up to and including the specified severity level. The severity level must be one of the following: **none**, **emerg**, **alert**, **crit**, **error**, **warning**, **notice**, **info**, **debug**.

`smcd -p` *`pid_file`*

Specify to use the given pid file instead of the default `/var/run/symantec/smcd.pid`. You should always use absolute path names when configuring smcd.

By default, /var/run/symantec/smcd.pid stores the process ID (pid) of the currently running copy of smcd. When smcd is terminated, this file is deleted.

`smcd -r` *`report_file`*

Specifies the use of a given report file instead of the default `/var/log/symantec/smcd_report.log`. You should always use absolute path names when configuring smcd.

`smcd -s` *`path`*

Set the working directory that the service runs in. You should always use absolute path names when configuring smcd.

This path typically does not need to be changed from the default, which is the root directory (/).

FILES

`/etc/sysconfig/smcd`

This configuration file specifies command-line options that are passed to the smcd program when it is started with the init.d script. To use this file, you must set the options to smcd between the quotes as shown in the following line:

```
SMCD_OPTS=""
```

For example, to log to the local0 facility and only log up to the error level of severity, you would use the following:

```
SMCD_OPTS="-f local0 -l error"
```

`/usr/etc/rc.d/init.d/smcd`

This file is the smcd 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 smcd daemon.

`/var/run/symantec/smcd.pid`

This file stores the process ID (pid) of the currently running smcd. When the currently running smcd service is terminated, this file is deleted.

symcfg

`symcfg` – The command-line interface for interacting with the configuration database for Symantec Endpoint Protection for Linux.

SYNOPSIS

```
symcfg [-q|--quiet] [-r|--recursive] command parameter(s)

symcfg [-h|--help]

symcfg add [-k|--key key [-v|--value value] [-d|--data data] [-t|--type type]]

symcfg delete [-k|--key key [-v|--value value]]

symcfg list [-k|--key [key|*] [-v|--value value]
```

DESCRIPTION

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 Endpoint Protection. 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 stored in this database.

You must have superuser privileges to use symcfg.

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

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

OPTIONS

`symcfg -q|--quiet` *`command parameter(s)`*

Display only the information that is requested; suppresses other information such as status and error messages. This option can be used with any other command and its parameters.

`symcfg -r|--recursive` *`command parameter(s)`*

Apply the command that follows recursively. This option can be used with any other command and its parameters.

`symcfg -h|--help`

Displays help information.

`symcfg add -k|--key key`

Mandatory. The name of the key that you want to add or overwrite. If no corresponding value is given, only the key is created.

`symcfg add -k -v|--value value`

The name of the key's value that you want to add or overwrite, which can be any string used as a registry entry.

`symcfg add -k -d|--data data`

The data that you want to store for the key's value/data pair, which can be any valid value for the corresponding data type.

`symcfg add -k -t|--type type`

One of the following constants for the key, representing the data type: **reg_sz** (string), **reg_dword** (32-bit unsigned integer), **reg_binary** (arbitrary binary data)

`symcfg delete -k|--key key`

Mandatory. The name of the key that you want to delete. If no corresponding value is given, the key and all of its values are deleted. If there are subkeys present and you do not delete them first, the delete fails.

`symcfg delete -k -v|--value value`

The name of the value that you want to remove.

`symcfg list -k|--key key`

Mandatory. The name of the key that you want to list. To list all keys from the root node, use an asterisk (*) instead of a key name. If used without the --value option, all subkeys and values for this key are listed.

You must escape an asterisk or put it in quotes to prevent it from being expanded by the shell.

`symcfg list -k -v|--value value`

The name of the value that you want to list. The value is displayed as the following:

`\\key\\subkey\\value_name value_data value_type`

symcfgd

`symcfgd` – The Symantec Endpoint Protection configuration service, which runs as a daemon process.

SYNOPSIS

`symcfgd [-Fchwx] [-f` *`log_facility`*`] [-k shutdown|report|check] [-l` *`log_severity`*`] [-p` *`pid_file`*`] [-r` *`report_file`*`] [-s` *`path`*`]`

DESCRIPTION

The symcfgd service runs as a daemon process and provides clients with access to a local registry database. This service is typically started automatically by the system initialization scripts. No changes to the defaults should be required.

You must have superuser privileges to use `symcfgd`.

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

OPTIONS

`symcfgd -F`

Run the service in the foreground. This option prevents the service from running as a daemon.

`symcfgd -c`

Write log entries also to the console (stderr).

`symcfgd -h`

Print help information to the standard output.

`symcfgd -w`

Wait for the debugger to be attached to the process.

`symcfgd -x`

Enable debug mode. Debug mode provides verbose logs and runtime checks.

`symcfgd -f` *`log_facility`*

Specify the log facility to use when logging to syslog. Possible values are **daemon**, **user**, and **local0** through **local7**. The default is **daemon**.

To set this up, you must also configure your `/etc/syslog.conf` file to specify handling for the facility.

`symcfgd -k shutdown`

Send a signal to the running copy of symcfgd to shut down, and then exit. The running copy is identified by a process with the pid that matches the pid stored in the pid file. The process attempts to perform a graceful shutdown.

When specifying the -k option and using a non-default pid file, the -p option 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.

`symcfgd -k report`

Send a signal to the running copy of symcfgd to report its status into a log file. The default log file is `/var/log/symantec/symcfgd_report.log`, but you can configure the log location with the -r option.

When specifying the -k option and using a non-default pid file, the -p option must also be given to ensure that the signal is sent to the correct smcd instance, even if there is only a single smcd instance running.

`symcfgd -k check`

Send a signal to the running copy of symcfgd to determine if symcfgd is currently running, print out a message, and exit. The running copy is identified by a process with the pid that matches the pid stored in the pid file. If there is a running copy, the command returns a 0. If there is no running copy, the command returns a 1.

When specifying the -k option and using a non-default pid file, the -p option 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.

`symcfgd -l` *`log_severity`*

Log all messages up to and including the specified severity level. The severity level must be one of the following: **none**, **emerg**, **alert**, **crit**, **error**, **warning**, **notice**, **info**, **debug**.

`symcfgd -p` *`pid_file`*

Specify to use the given pid file instead of the default `/var/run/symantec/symcfgd.pid`. 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.

`symcfgd -r` *`report_file`*

Specifies the use of a given report file instead of the default `/var/log/symantec/symcfgd_report.log`. You should always use absolute path names when configuring smcd.

`symcfgd -s` *`path`*

Set the working directory that the service runs in. You should always use absolute path names when configuring symcfgd.

This typically does not need to be changed from the default, which is the root directory (/).

FILES

`/etc/sysconfig/symcfgd`

This configuration file specifies command-line options that are passed to the symcfgd program when it is started with the init.d script. To use this file, you must set the options to symcfgd between the quotes as shown 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.