Symantec™ Endpoint Protection 14.3 RU3 for Linux Client Guide

September 2021

Table of Contents

Copyright statement

Protecting Linux devices with Symantec Endpoint Protection

About the Symantec Agent for Linux

Symantec Agent for Linux protects your Linux devices from malware threats, risks, and vulnerabilities. It proactively secures your Linux devices against known and unknown malwares.

The antimalware features consist of **Antimalware** (AMD) that protects your Linux devices from malicious software, such as viruses, spyware, ransomware etc., and **Auto-Protect** (AP) that detects malicious threats when an application is launched.

Symantec recommends to have auto-protect enabled to ensure the real-time protection. Any malware that is detected is immediately quarantined. If you disable auto-protect, you can still detect malware using an on-demand scan.

Getting started on the Linux agent

Symantec Agent for Linux system requirements

This section includes the system requirements for the most current version.

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: Symantec Agent for Linux system requirements

Component	Requirements
Hardware	• Intel Pentium 4 (2 GHz) or later processor • 500 MB of free RAM (4 GB of RAM is recommended) • 2 GB available disk space if `/var`, `/opt`, and `/tmp` share the same filesystem/volume • 500 MB available disk space in each `/var`, `/opt`, and `/tmp` if on different volumes
Operating systems	• Amazon Linux 2 • CentOS 6, 7, 8 • Debian 9, 10 • Oracle Enterprise Linux 6, 7, 8 • Red Hat Enterprise Linux 6, 7, 8 • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS For a list of supported operating system kernels, see Supported Linux kernels for Symantec Endpoint Protection.

Installing the Symantec Linux Agent or the Symantec Endpoint Protection client for Linux

(For 14.3 RU1 and later)

You install Symantec Linux Agent directly on a Linux device. You cannot deploy the Linux agent from Symantec Endpoint Protection Manager remotely.

To install Symantec Linux Agent, create an installation package in Symantec Endpoint Protection Manager, transfer the installation package to a Linux device and then run the installer. The installer will configure the new agent and register it with Symantec Endpoint Protection Manager.

> **NOTE**
> Symantec Linux Agent 14.3 RU1 and later cannot run as an unmanaged client. All management tasks must be performed in Symantec Endpoint Protection Manager or in the cloud console.

(For 14.3 RU1 and later) To install the Symantec Linux Agent:

1. In Symantec Endpoint Protection Manager, create and download the installation package.
2. Put the package on a network share, USB device, or other share mechanism.
   If the devices where you want to install the Linux agent are in an isolated network or do not have Internet access, configure a local repository. See:
   Creating a local repository
3. Install the Linux agent in one of the following ways:

If you transferred the package to the Linux device	1. Navigate to folder location and run the following command to make the **LinuxInstaller** file executable:
	`chmod u+x LinuxInstaller`
	2. Run the following command to install the agent:
	`./LinuxInstaller`

If you configured a local repository	1. Run the following command:
	`./LinuxInstaller – --local-repo <LOCAL Repository URL>`
	For example:
	`./LinuxInstaller – --local-repo https://your-domain.com/sep_linux_agent/14_3RU3`

   You must run the command as root.
   To view the list of installation options, run `./LinuxInstaller -h`.
4. To verify the installation, navigate to `/usr/lib/symantec` and run `./status.sh` to confirm that the modules are loaded and daemons are running:

```
./status.sh
Symantec Agent for Linux Version: 14.3.450.1000
Checking Symantec Agent for Linux (SEPM) status..
Daemon status:
cafagent              running
sisamdagent           running
sisidsagent           running
sisipsagent           running
Module status:
sisevt                loaded
sisap                 loaded
```

   Note that `communication status` is only available for cloud-managed clients.

(For 14.3 MP1 and earlier)

You install an unmanaged or managed Symantec Endpoint Protection client directly on a Linux computer. You cannot deploy the Linux client from Symantec Endpoint Protection Manager remotely. The installation steps are similar whether the client is unmanaged or managed.

The only way to install a managed client is with an installation package that you create in Symantec Endpoint Protection Manager. You can convert an unmanaged client to a managed client at any time by importing client-server communication settings into the Linux client.

If the Linux operating system kernel is incompatible with the pre-compiled Auto-Protect kernel module, the installer tries to compile a compatible Auto-Protect kernel module. The auto-compile process automatically launches if it is needed. However, the installer might be unable to compile a compatible Auto-Protect kernel module. In this case, Auto-Protect installs but is disabled. For more information, see:

Supported Linux kernels for Symantec Endpoint Protection

NOTE

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

(For 14.3 MP1 and earlier) To install the Symantec Endpoint Protection client for Linux:

1. Copy the installation package that you created to the Linux computer. The package is a .zip file.
2. On the Linux computer, open a terminal application window.
3. Navigate to the installation directory with the following command:

   ```
   cd /directory/
   ```

   Where directory is the name of the directory into which you copied the .zip file.
4. Extract the contents of the .zip file into a directory named `tmp` with the following command:

   ```
   unzip "InstallPackage" -d sepfiles
   ```

   Where `InstallPackage` is the full name of the .zip file, and `sepfiles` represents a destination folder into which the extraction process places the installation files.

   If the destination folder does not exist, the extraction process creates it.
5. Navigate to `sepfiles` with the following command:

   ```
   cd sepfiles
   ```
6. To correctly set the execute file permissions on `install.sh`, use the following command:

   ```
   chmod u+x install.sh
   ```
7. Use the built-in script to install Symantec Endpoint Protection with the following command:

   ```
   sudo ./install.sh -i
   ```

   Enter your password if prompted.

   This script initiates the installation of the Symantec Endpoint Protection components. The default installation directory is as follows:

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

   The default work directory for LiveUpdate is as follows:

   ```
   /opt/Symantec/LiveUpdate/tmp
   ```

   The installation completes when the command prompt returns. You do not have to restart the computer to complete the installation.

(For 14.3 MP1 and earlier)

To verify the client installation, click or right-click the Symantec Endpoint Protection yellow shield and then click **Open Symantec Endpoint Protection**. The location of the yellow shield varies by Linux version. The client user interface displays information about program version, virus definitions, server connection status, and management.

More information

Getting started on the Linux agent

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

Table 2: Steps to get started on the Linux agent (for 14.3 RU1 and later)

Step	Task	Description
Step 1	Install the Symantec Agent for Linux.	The administrator provides you with the installation package for a managed client or sends you a link by email to download it. See: Installing the Symantec Linux Agent or the Symantec Endpoint Protection client for Linux
Step 2	Check that the Linux agent communicates with the Symantec Endpoint Protection Manager or cloud console.	To confirm the connection to Symantec Endpoint Protection Manager or cloud console, you can run the following command: `/usr/lib/symantec/status.sh`
Step 3	Verify that the Auto-Protect is running.	To check the status of Auto-Protect, run the following command: `cat /proc/sisap/status`
Step 4	Check that the definitions are up to date.	LiveUpdate definitions are available at the following location: `/opt/Symantec/sdcssagent/AMD/sef/definitions/`

Table 3: Steps to get started on the Linux client (for 14.3 MP1 and earlier)

Step	Task	Description
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: Installing the Symantec Linux Agent or the Symantec Endpoint Protection client for Linux
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.
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`
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`

Step	Task	Description
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.

More information

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

Upgrading the Symantec Linux Agent

(For 14.3 RU1 and later)

As of version 14.3 RU1, the Linux client installer detects and uninstalls the legacy Linux client (earlier than 14.3 RU1) and then performs a fresh install. Old configurations will not be retained.

To upgrade the Symantec Linux Agent:

1. In Symantec Endpoint Protection Manager, create and download the installation package.
2. Copy the downloaded package to the Linux device.
3. Navigate to folder location and run the following command to make the **LinuxInstaller** file executable:

   ```
   chmod u+x LinuxInstaller
   ```
4. Run the following command to uninstall the existing agent and re-install the Symantec Linux Agent:

   ```
   ./LinuxInstaller
   ```

   Run the command as root.
5. To verify the installation, navigate to `/usr/lib/symantec` and run `./status.sh` script to confirm that the modules are loaded and daemons are running:

   ```
   ./status.sh
   Symantec Agent for Linux Version: 14.3.450.1000
   Checking Symantec Agent for Linux (SEPM) status..
   Daemon status:
   cafagent              running
   sisamdagent           running
   sisidsagent           running
   sisipsagent           running
   Module status:
   sisevt                loaded
   sisap                 loaded
   ```

Updating the kernel modules for the Symantec Linux Agent

(For 14.3 RU1 and later)

Whenever a new Linux kernel update is released, the Symantec Linux Agent for that platform needs to be updated to support the new kernel. To make the process more efficient, the kernel modules of the Linux agent can now be updated by using the Linux repository.

> **NOTE**
> Ensure that the agents can connect to the Symantec repository server (https://linux-repo.us.securitycloud.symantec.com/) to download the kernel module updates.

Whenever you run the `yum update` command on a RHEL, Amazon Linux, Oracle Linux, or CentOS system, the command also looks for new agent packages. If an update is available, the latest kernel module is downloaded and the agent is updated automatically. After the kernel module is updated, you must restart the instance for the update to take effect.

Alternatively, you can update the agent kernel module by running the following command in the instance. Open a terminal window with root privileges, navigate to `/usr/lib/symantec/` and run the following command:

```
/usr/lib/symantec/installagent.sh --update-kmod
```

For the Ubuntu systems, type the following commands:

1. To refresh and update local package database:
   ```
   sudo apt-get clean
   sudo apt-get update
   ```
2. To upgrade to the latest kernel module:
   ```
   /usr/lib/symantec/installagent.sh --update-kmod
   ```
   Superuser privileges are required to perform this action.

In a restricted environment with no Internet connection, you can update the kernel modules in one of the following ways:

1. Manually transfer the latest KMOD package to a system that has no Internet connection, attach the KMOD package to the LinuxInstaller, and then run the LinuxInstaller.
   1. On a system that has Internet connection, download the KMOD package.
      ```
      ./LinuxInstaller -d
      ```
   2. Manually copy and paste the KMOD package to the agent that you want to upgrade.
   3. List the attached packages.
      ```
      ./LinuxInstaller -l
      ```
   4. Attach the new KMOD package to the LinuxInstaller.
      ```
      tar czf - [KMOD-package-name] >> LinuxInstaller
      ```
   5. Make sure that the new KMOD package is included in the list of attached packages.
      ```
      ./LinuxInstaller -l
      ```
   6. Run the installer to update the kernel modules.
      ```
      ./LinuxInstaller -- --update-kmod
      ```
2. Set up a local repository and edit the repository settings so that the agent uses the local repository instead of the default Symantec repository.
   1. Set up the local repository that hosts the KMOD packages.
      For information about how to create a local repository, refer to documentation of the respective Linux distribution that you are using.
   2. On the client computer, run the following command to redirect it to use the local repo:
      ```
      ./LinuxInstaller --local-repo <localrepo_url>
      ```
      Example of the URL: `--local-repo 'http://<repo_ip_or_hostname:<port_optional>/sep_linux'`
   3. To update the KMOD, run:
      ```
      ./LinuxInstaller -- --update-kmod
      ```

If you update the operating system kernel modules, you must also update the corresponding kernel module update for the Symantec Endpoint Protection client. Without the compatible kernel modules, the Symantec Endpoint Protection client may not work properly and some features may be disabled.

Managing your Linux client using the command line tool (sav)

(For 14.3 RU2 and later)

The Linux client command line tool lets you control and check on your Linux client.

To manage your Linux client using the command line tool

1. On a Linux client computer, navigate to the following location:
   `/opt/Symantec/sdcssagent/AMD/tools`
2. Run the sav command as follows:
   `./sav [options] command`

Table 4: Options for sav

Option	Description	Applies to
`-q`	Quiet	As of 14.3 RU2
`-h`	Displays available options and commands for sav.	As of 14.3 RU2

Table 5: Commands for sav

Option	Description	Applies to
`autoprotect -e`	Enables Auto-Protect. To check the Auto-Protect status, run the following command: `[root@localhost tools]# cat /proc/sisap/status | grep -i MODE` The reply can be one of the following: • `mode=ENA` (if enabled) • `mode=DIS` (if disabled)	As of 14.3 RU2
`autoprotect -d`	Disables Auto-Protect.	As of 14.3 RU2
`info -d`	Shows the version and date of the current virus and security risk definitions in use on the device.	As of 14.3 RU3
`info -e`	Shows the version of the scan engine in use on the device.	As of 14.3 RU3
`info -p`	Shows the Symantec Agent version in use on the device.	As of 14.3 RU3
`info -a`	Shows the status of Auto-Protect on the device.	As of 14.3 RU3
`liveupdate -u`	Runs LiveUpdate immediately.	As of 14.3 RU3
`manage -i <file>`	Imports the *sylink.xml* file to the specified location.	As of 14.3 RU2
`manualscan -s <file list>`	Starts a manual scan. <file list> 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 started 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. 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.	As of 14.3 RU3
`manualscan -t`	Stops a manual scan that is in progress.	As of 14.3 RU3

More information

Troubleshooting the Symantec Linux Agent

Troubleshooting the Symantec Linux Agent

In the table below you find the resources for troubleshooting the Symantec Linux Agent (as of 14.3 RU1).

Action	Description
Checking the status of the agent.	To check the version and connection status of the agent and to confirm that the modules are loaded and daemons are running, navigate to `/usr/lib/symantec` and run the following command: `./status.sh`
Checking the versions of the agent packages.	Navigate to `/usr/lib/symantec` and run the following command: `./version.sh`

Viewing the logs.	You find the Symantec Linux Agent logs at the following locations:
	• AMD log - provides information related to scanning.
	`/var/log/sdcsslog/amdlog`
	• CAF log - provides information related to agent activities such as communication with the server, enrollment, commands, events, etc.
	`/var/log/sdcss-caflog/`
	• Agent log - provides information related to agent activities.
	`/var/log/sdcsslog/SISIDSEvents*.csv`
	• CVE log - provides information related to communication between Symantec Endpoint Protection Manager and the agent.
	`/var/log/sdcss-caflog/cve.log`

Collecting the logs into a zip file.	You can use `GetAgentInfo` script to collect all log files into a ZIP file that you can send to customer support. 1. Login to Symantec Linux Agent system. 2. Navigate to `/opt/Symantec/sdcssagent/IPS/tools/`. 3. Run `./getagentinfo.sh` as root. 4. A ZIP file will be created in `/tmp/` directory. The name of the file will look similar to `20201208_184935_0001_CU_mihsan-rhel8.zip` `-out <directory>` lets you change the location and the name of the generated ZIP file.
Changing the CVE logging level.	By default, the CVE logging level is `info`. You can change the logging level to `debug` in the `/opt/Symantec/cafagent/bin/log4j.properties` file. After changing the file, you must restart the `cafagent` service.
Changing the AMD logging level.	By default, the AMD logging level is `info`. You can change the logging level to `trace`, to `warning`, or to `error` in the `/opt/Symantec/sdcssagent/AMD/system/AntiMalware.ini` file. **Note:** Before you modify the AntiMalware.ini file, stop the sisamdagent: **Note:** `service sisamdagent stop` **Note:** After you modify the file, restart the service: **Note:** `service sisamdagent start`

Uninstalling the Symantec Linux Agent or 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.

(For 14.3 RU1 and later) To uninstall the Symantec Linux Agent:

1. On the Linux computer, open a terminal application window.
2. Navigate to the following directory:
   `/usr/lib/symantec/`
3. Run the following built-in script to uninstall Symantec Agent for Linux:
   `./uninstall.sh`
4. Reboot the computer after the uninstallation finishes and the reboot prompt appears.
   Note that the `uninstall.sh` script will remove all components of Symantec Agent for Linux (`sdcss-caf`, `sdcss-sepagent`, and `sdcss-kmod`).

```
[root@localhost symantec]# ./uninstall.sh
Running ./uninstall.sh (PWD /usr/lib/symantec; version 2.2.4.41)
Uninstalling Symantec Agent for Linux (SEPM) ...
Removing packages sdcss-caf sdcss-sepagent sdcss-kmod sdcss-scripts
Symantec Agent for Linux (SEPM) uninstalled successfully.
A reboot is required to complete uninstallation.
Please reboot your machine at the earliest convenience.
```

(For 14.3 MP1 and earlier) 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.


Symantec
A Division of Broadcom