Symantec ™ Endpoint Protection 14.3 RU1 for Linux Client Guide

December 2020

Table of Contents

Copyright statement

Copyright statement

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

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 • 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.
Other environmental requirements	• Glibc Any operating system that runs glibc earlier than 2.6 is not supported. • net-tools or iproute2 Symantec Endpoint Protection uses one of these two tools, depending on what is already installed on the computer. • OpenSSL 1.0.2k-fips or later

Installing the Symantec Agent for Linux 14.3 RU1

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

To install Symantec Agent for Linux, 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 Agent for Linux 14.3 RU1 cannot run as an unmanaged client. All management tasks must be performed in Symantec Endpoint Protection Manager or in cloud console.

System requirements for Symantec Endpoint Protection (SEP) 14.3 RU1

To install the Symantec Management Agent for Linux 14.3 RU1

1. In Symantec Endpoint Protection Manager, create and download the installation package.

   Exporting client installation packages
2. Move the `LinuxInstaller` package to a Linux device.
3. Make the `LinuxInstaller` file executable:

   ```
   chmod u+x LinuxInstaller
   ```
4. Run the installer:

   ```
   ./LinuxInstaller
   ```

   You must run the command as root.

   To view the list of installation options, run `./LinuxInstaller -h`.
5. 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.

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 (as of version 14.3 RU1)

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. Installing the Symantec Agent for Linux 14.3 RU1
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 (version 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. Installing the Symantec Endpoint Protection client for Linux Importing client-server communication settings into the Linux client
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. About the Linux client graphical user interface
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 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.

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

Upgrading to the Symantec Agent for Linux 14.3 RU1

Symantec Agent for Linux 14.3 RU1 detects and uninstalls the older Symantec Endpoint Protection client for Linux and then performs a fresh install. Old configurations will not be retained.

To upgrade to the Symantec Agent for Linux 14.3 RU1

1. In Symantec Endpoint Protection Manager, create and download the installation package.

   Exporting client installation packages

2. Move the `LinuxInstaller` package to a Linux device.
3. Make the `LinuxInstaller` file executable:

   ```
   chmod u+x LinuxInstaller
   ```

4. Start the installation of the new 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 Agent for Linux

Whenever a new Linux kernel update is released, the Symantec Agent for Linux 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 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 privilege, 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.

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.

https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/getting-up-and-running-on-for-the-first-time-v45150512-d43e1033/installing-clients-with-save-package-v16194723-d21e1502/Installing-Symantec-Agent-for-Linux-14-3-RU1.html

Troubleshooting Symantec Agent for Linux

In the table below you find the resources for troubleshooting the Symantec Agent for Linux (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 Agent for Linux 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 Agent for Linux 14.3 RU1 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 `ebug` in the `/opt/Symantec/cafagent/bin/log4j.properties` file. After changing the file, you must restart the `cafagent` service.

Action	Description
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. After changing the file, you must restart the service.

Symantec™

A Division of Broadcom