Symantec™ Endpoint Protection 14.3 Release Notes

Last updated: July 8, 2020

Table of Contents

Copyright statement

What's new for Symantec Endpoint Protection 14.3?

This section describes the new features for the 14.3 release.

Protection Features

- Third-party application developers can protect their customers from dynamic script-based malware and from non-traditional avenues of cyberattack. The third-party application calls the Windows AMSI interface to request a scan of user-provided script, which is routed to the Symantec Endpoint Protection client. The client responds with a verdict to indicate on whether or not the script behavior is malicious. If the behavior is not malicious, then the script execution proceeds. If the script's behavior is malicious, the application does not run it. On the client, the Detection Results dialog box displays a status of "Access Denied." Examples of third-party scripts include Windows PowerShell, JavaScript, and VBScript. Auto-Protect must be enabled. This functionality works for Windows 10 and later computers.
  How the Antimalware Scan Interface (AMSI) helps you defend against malware
  Antimalware Scan Interface (AMSI)

Symantec Endpoint Protection Manager

- The Symantec Endpoint Protection remote console now supports Java 11 instead of Java 8. To access the remote console, open a supported web browser and type the following address in the address box: `http://SEPMServer:9090/symantec.html` and download new remote console package. Follow the instructions mentioned. The previous version of the Symantec Endpoint Protection Manager remote console is no longer supported.
  Logging on to Symantec Endpoint Protection
- You can configure one of the Symantec Endpoint Protection Managers on the site as a master logging server to forward logs to the syslog server. If the master logging server goes offline, a second management server takes over and forwards logs to the syslog server. When the master logging server comes back online, it resumes forwarding the logs.
  Configuring a failover server for external logging
- The Integrations policy has a new option for WSS Traffic Redirection, **Enable LPS Custom PAC file**. This option lets you replace the default PAC file that is hosted by the LPS server on the client with a custom PAC file. The custom PAC file solves compatibility issues with third-party applications that do not work with a local proxy server listening on the loopback adapter.
  Configuring WSS Traffic Redirection
- Support for the Microsoft SQL Server 2019 database.
- The antivirus scan process now uses a separate service from the main non-security service. This new scan process brings more efficient memory usage, continual protection, and less dependency on issues with the main service.
  Endpoint Protection 14.3 scan process separation
- The database schema includes new columns as part of a feature for a future release. (AGENT_SECURITY_LOG_1, AGENT_SECURITY_LOG_2, SEM_AGENT tables)
- The Rest API has the following fields in the /sepm/api/v1/computers API response JSON to call and download the Computer Status report: quarantineStatus, quarantineCode, wssStatus, pskVersion.
- Upgraded the following third-party components to newer versions: Apache Tomcat, Boost C++ Libraries, cURL, Jackson-core, jackson-databind, Jakarta Activation, Java, logback, Microsoft JDBC Driver for SQL Server, OpenSC, OpenSSL, Spring Security, spring-framework, sqlite.
- To enroll the Symantec Endpoint Protection Manager domain in the cloud console, you must first get the enrollment token through the Symantec Endpoint Security console. Previously, you got the enrollment token by clicking **Get Started** on the **Cloud** page.

Client and platform updates

- The Windows client supports Windows 10 20H1 (Windows 10 version 2004)
- The Linux client now supports Ubuntu 18.04, RHEL 8, and CentOS 8.
- The AppRemover tool was updated to a newer version. The AppRemover tool removes third-party applications before you can install the Windows client. For more information on which applications it removes, see: Third-party security software removal in Endpoint Protection 14.3

Features Removed

- The following notifications no longer show the **Risk severity** and **Risk type** fields: Risk Outbreak, Single Risk Event, New Risk Detected.

What's new in all releases of Symantec Endpoint Protection

Known issues and workarounds

The items in this section apply to this release of Symantec Endpoint Protection.

Table 1: Upgrade issues

Issue	Description and solution
A SQL Server upgrade from version 2017 to version 2019 fails with FIPS mode enabled [14.3]	You may see the error: "The following error has occurred. An error occurred while installing extensibility feature with error message: AppContainer Creation Failed with error message NONE, state. This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms." This occurs if you have a FIPS-enabled Symantec Endpoint Protection Manager 14.3 and you upgrade from the Microsoft SQL Server 2017 to 2019. [SEP-61473] To work around this issue, disable FIPS at the operating system level: 1. In `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools`, click **Local Security Policy** > **Local Policies** > **Security Options**, and disable **System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing** 2. Upgrade from SQL Server version 2017 to version 2019. 3. After SQL Server upgrades successfully, re-enable FIPS. SQL upgrade from 2017 to 2019 fails with FIPS mode enabled
Custom names may prevent the firewall policy from updating during an upgrade to 14.2 or later	For an upgrade to Symantec Endpoint Protection 14.2 or later, firewall policies cannot incorporate the changes for IPv6 if you changed some default names. The default names include the names of default policies and default rule names. If the rules cannot be updated during the upgrade, the IPv6 options do not appear. Any new policies or rules that you create after the upgrade are not affected. If possible, revert any changed names back to the default. Otherwise, ensure that any custom rules that you added to a default policy do not block IPv6 communication in any way. Ensure the same for any new policies or rules that you add.

Table 2: Symantec Endpoint Protection Manager issues

Issue	Description and solution
Whitelist additional URLs in Symantec Endpoint Security if you use the hybrid management option and proxy servers [14.2.2.1 or later]	With Broadcom's recent acquisition of Symantec Enterprise Security, the URLs for client-to-cloud communication changed in 14.2.2.1. [CDM-42467] You must upgrade your clients to version build 14.2.5569.2100 or later in the following situation • You use Symantec Endpoint Security to manage your clients and policies when your on-premises Symantec Endpoint Protection Manager domains are enrolled in the cloud console • You use proxy servers. To whitelist URLs in either fully cloud-managed or hybrid-managed agents, you whitelist them in Symantec Endpoint Security: 1. In Symantec Endpoint Security, go to **Endpoint > Policies > [policy name] Whitelist Policy**. 2. In the Whitelist policy, next to **Excluded by Domain**, select **Add**, add the following URLs one at a time, and select **Add**: `us.spoc.securitycloud.symantec.com` `eu.spoc.securitycloud.symantec.com` (add if you have devices in Europe). Keep spoc.norton.com if you continue to manage clients with a later version. 3. Select **Save Policy** and then **Yes** to update the policy and apply it to existing groups. See URLs to whitelist for Symantec Endpoint Security. See Upgrade cloud-managed Symantec Agents to version 14.2 RU2 MP1 or later.
The Symantec Endpoint Protection Manager remote console no longer supports the 32-bit Windows platform [14.3]	As of 14.3, you cannot log on to the Symantec Endpoint Protection Manager remote console if you run a 32-bit version of Windows. The Oracle Java SE Runtime Environment no longer supports 32-bit versions of Microsoft Windows. [SEP-61106] If you see the following message, log on to Symantec Endpoint Protection Manager locally: "This version of C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe is not compatible with the version of Windows you're running. Check your computer's system information and then contact the software publisher." Logging on to the Symantec Endpoint Protection Manager
"Failed to install Microsoft Visual C++ Runtime" error appears while you install Symantec Endpoint Protection Manager [14.3]	You may see the following error while installing the Symantec Endpoint Protection Manager on Windows 2012 R2: "Failed to install Microsoft Visual C++ Runtime" [SEP-60396] To work around this issue, activate Windows and install the Windows updates. The Windows update installs the Visual C++ 2017 redistributable, which is a prerequisite for the Symantec Endpoint Protection Manager 14.3 installation on Windows 2012 R2.
Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows [14.3]	After you upgrade to or install a Symantec Endpoint Protection Manager version 14.3 that is enrolled in the cloud console, the management server no longer uploads logs successfully to the cloud. In the uploader.log you may see the following error: `<SEVERE> WinHttpSendRequest: 12175: A security error occurred` This issue is caused by a missing Microsoft update that provides support for TLS 1.1 and 1.2. To solve the issue, install Microsoft update: KB3140245. For more information, see: Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows
"Deployment in progress" still appears in Symantec Endpoint Protection Manager after the client receives an updated policy for Endpoint Threat Defense for AD [14.2 RU1 MP1 and later]	This behavior is expected. Endpoint Threat Defense for AD 3.3 policies are only supported on the client as of version 14.2 RU1 MP1. You apply a policy for Symantec Endpoint Threat Defense for Active Directory 3.3 to a group. This group contains some clients that run Symantec Endpoint Protection 14.2 RU1 or earlier. These clients receive and apply the policy as expected, but the status in Symantec Endpoint Protection Manager continues to show the message Deployment in progress.

Table 3: Windows, Mac, and Linux client issues

Issue	Description and solution
The Symantec Endpoint Protection 14.3 Windows client installation may fail unless you first install SHA-2 support [14.3]	If you run legacy operating system versions (Windows 7 RTM or SP1, Windows Server 2008 R2 or R2 SP1 or R2 SP2), you are required to have SHA-2 code signing support installed on your devices to install Windows updates released on or after July 2019. Without SHA-2 support, the Windows client installation sometimes fails. The installation may fail whether you install clients for the first time or automatically upgrade from a previous release. [SEP-61175/61403] To get Microsoft enforced SHA-2 code signing support, see: 2019 SHA-2 Code Signing Support requirement for Windows and WSUS Symantec Endpoint Protection 14.3 Windows client may fail to install unless SHA-2 support is installed
The Symantec Endpoint Protection Windows client does not run when installed on Windows 10 1803 with UWF enabled [14.3]	If the Symantec Endpoint Protection client runs on the Windows 10 RS4 1803 32-bit operating system when the Unified Write Filter (UWF) is enabled and protecting the drive on which the Windows client is installed, the client does not run properly. This Windows operating system contains a UWF defect that prevents the Windows client from running. To work around this issue: • Upgrade to another operating system version that does not contain the defect. • Disable UWF. See: Endpoint Protection is malfunctioning when installed on Windows 10 1803 with UWF enabled
Mac clients that enable WSS Traffic Redirection do not honor custom proxy settings for LiveUpdate [14.2 RU1 MP1 and later]	You have configured your managed Mac clients for Symantec Endpoint Protection 14.2 RU1 MP1 or later to use custom proxy settings for LiveUpdate through External Communications Settings. After you enable WSS Traffic Redirection (WTR) for your Mac clients through the Symantec Endpoint Protection Manager policy, however, you find that LiveUpdate traffic no longer honors your custom proxy settings. Instead, LiveUpdate attempts a direct connection. To work around this issue, only use custom proxy settings for LiveUpdate when WSS Traffic Redirection is disabled.
Microsoft Edge unexpectedly allows PDF downloads with Hardening enabled [14.2 RU1 MP1 and later]	With Application Hardening enabled in the Symantec Endpoint Protection client, you are unexpectedly able to download PDF files if you use the Microsoft Edge browser. The prevention of the download of PDF files works as expected with other browsers. A fix for this issue is planned for a future release.

With Broadcom's recent announcement that Symantec Enterprise Protection has officially joined Broadcom, Symantec migrated the documentation to the Broadcom Symantec Security Tech Docs Portal.

To find Endpoint Protection documentation, click the **Symantec Security Software** tab, then click **Endpoint Security and Management** > **Endpoint Protection**.

Table 4: Documentation issues

Issue	Description and solution
HOWTO articles have been expired.	The HOWTO articles, which were duplicates of the topics in the Symantec Endpoint Protection Manager Help, have been republished on the Endpoint Protection site and now have a different URL. To find an article, use the **Search field**.
PDF files	Symantec posted all PDF files on DOC articles. These pages have been expired. To find the release most recent version of the PDF file, go to the Related Documents page. In the future, Broadcom will be adding legacy PDF files and translated PDF files.

For resolved issues, see: New fixes and components for Symantec Endpoint Protection 14.3

System requirements for Symantec Endpoint Protection (SEP)

In general, the system requirements for the following are the same as those of the operating systems on which they are supported.

> **NOTE**
> An earlier version of Symantec Endpoint Protection Manager may not be able to correctly manage a client with a later version. Issues with content updates and client management may occur. For example, Symantec Endpoint Protection Manager 14.0.1 or earlier cannot correctly provide a version 14.2 client with its version-specific monikers. Symantec Endpoint Protection Manager for versions earlier than 14 MP2 cannot correctly provide client versions later than 14.0.1 with their version-specific monikers.

The following tables describe the software and hardware requirements for Symantec Endpoint Protection.

Table 5: Symantec Endpoint Protection Manager (SEPM) software system requirements

Component	Requirements
Operating system	• Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **Note:** Desktop operating systems are not supported. **Note:** Windows Server Core edition is not supported. Windows Server Core does not include Internet Explorer, which Symantec Endpoint Protection Manager requires to work.
Web browser	The following browsers are supported for web console access to Symantec Endpoint Protection Manager and for viewing the Symantec Endpoint Protection Manager Help: • Microsoft Edge Note: The 32-bit version Windows 10 does not support web console access on the Edge browser. • Microsoft Internet Explorer 11 • Mozilla Firefox 5.x through 68.x • Google Chrome 75.x

Component	Requirements
Database	**The Symantec Endpoint Protection Manager includes an embedded database. You may instead choose to use a database from one of the following versions of Microsoft SQL Server:** • SQL Server 2008, SP4 • SQL Server 2008 R2, SP3 • SQL Server 2012, RTM - SP4 • SQL Server 2014, RTM - SP3 • SQL Server 2016, RTM, SP1, SP2 • SQL Server 2017, RTM • SQL Server 2019, RTM (as of 14.3) **Note:** The SQL Server Express Edition database is not supported. SQL Server databases that are hosted on Amazon RDS are supported (As of 14.0.1 MP2). **Note:** If Symantec Endpoint Protection uses a SQL Server database and your environment only uses TLS 1.2, ensure that SQL Server supports TLS 1.2. You may need to patch SQL Server. This recommendation applies to SQL Server 2008, 2012, and 2014. Without the SQL Server patch to support TLS 1.2, you may have issues when you upgrade from Symantec Endpoint Protection 12.1 to 14. **Note:** TLS 1.2 support for Microsoft SQL Server
Other environmental requirements	In purely IPv6 networks, the IPv4 stack must still be installed and disabled. If the IPv4 stack is uninstalled, Symantec Endpoint Protection Manager does not work.

Table 6: Symantec Endpoint Protection Manager hardware system requirements

Component	Requirements
Processor	Intel Pentium Dual-Core or equivalent minimum, 8-core or greater recommended **Note:** Intel Itanium IA-64 processors are not supported.
Physical RAM	2 GB RAM available minimum; 8 GB or more available recommended **Note:** Your Symantec Endpoint Protection Manager server may require additional RAM depending on the RAM requirements of other applications that are already installed. For example, if Microsoft SQL Server is installed on the Symantec Endpoint Protection Manager server, the server should have a minimum of 8 GB available.
Display	1024 x 768 or larger
Hard drive when installing to the system drive	**With an embedded database or a local SQL Server database:** • 40 GB available minimum (200 GB recommended) for the management server and database **With a remote SQL Server database:** • 40 GB available minimum (100 GB recommended) for the management server • Additional available disk space on the remote server for the database
Hard drive when installing to an alternate drive	**With an embedded database or a local SQL Server database:** • The system drive requires 15 GB available minimum (100 GB recommended) • The installation drive requires 25 GB available minimum (100 GB recommended) **With a remote SQL Server database:** • The system drive requires 15 GB available minimum (100 GB recommended) • The installation drive requires 25 GB available minimum (100 GB recommended) • Additional available disk space on the remote server for the database

If you use a SQL Server database, you may need to make more disk space available. The amount and location of additional space depends on which drive SQL Server uses, database maintenance requirements, and other database settings.

Table 7: Symantec Endpoint Protection client for Windows software system requirements

Component	Requirements
Operating system (desktop)	• Windows 7 (32-bit, 64-bit; RTM and SP1) • Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit and 64-bit) • Windows 8 (32-bit, 64-bit) • Windows Embedded 8 Standard (32-bit and 64-bit) • Windows 8.1 (32-bit, 64-bit), including Windows To Go • Windows 8.1 update for April 2014 (32-bit, 64-bit) • Windows 8.1 update for August 2014 (32-bit, 64-bit) • Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit and 64-bit) • Windows 10 (version 1507) (32-bit, 64-bit), including Windows 10 Enterprise 2015 LTSB • Windows 10 November Update (version 1511) (32-bit, 64-bit) • Windows 10 Anniversary Update (version 1607) (32-bit, 64-bit), including Windows 10 Enterprise 2016 LTSB • Windows 10 Creators Update (version 1703) (32-bit, 64-bit) • Windows 10 Fall Creators Update (version 1709) (32-bit, 64-bit) • Windows 10 April 2018 Update (version 1803) (32-bit, 64-bit) • Windows 10 October 2018 Update (version 1809) (32-bit, 64-bit), including Windows 10 Enterprise 2019 LTSC. • Windows 10 May 2019 Update (version 1903) (32-bit, 64-bit) • Windows 10 November 2019 Update (version 1909) (32-bit, 64-bit) (14.2 RU1 and later) • Windows 10 20H1 (Windows 10 version 2004) (as of 14.3)
Operating system (server)	• Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2012 R2 update for April 2014 • Windows Server 2012 R2 update for August 2014 • Windows Server 2016 • Windows Server 2019 • Windows Server, version 1803 (Server Core) (14.2 and later) • Windows Server, version 1809 (Server Core) • Windows Server, version 1903 (Server Core) (14.2 RU1 and later) • Windows Server, version 1909 (Server Core) (14.2 RU1 and later)
Browser Intrusion Prevention	Browser Intrusion Prevention support is based on the version of the Client Intrusion Detection System (CIDS) engine. See Supported browsers for Browser Intrusion Prevention in Endpoint Protection.

Table 8: Symantec Endpoint Protection client for Windows hardware system requirements

Component	Requirements
Processor (for physical computers)	• 32-bit processor: 2 GHz Intel Pentium 4 or equivalent minimum (Intel Pentium 4 or equivalent recommended) • 64-bit processor: 2 GHz Pentium 4 with x86-64 support or equivalent minimum **Note:** Itanium processors are not supported.
Processor (for virtual computers)	One virtual socket and one core per socket at 1 GHz minimum (one virtual socket and two cores per socket at 2 GHz recommended) **Note:** The hypervisor resource reservation must be enabled.
Physical RAM	1 GB (2 GB recommended) or higher if required by the operating system
Display	800 x 600 or larger
Hard drive	Disk space requirements depend on the type of client you install, which drive you install to, and where the program data file resides. The program data folder is usually on the system drive in the default location C:\ProgramData. Available disk space is always required on the system drive, regardless of which installation drive you choose. **Note:** Space requirements are based on NTFS file systems. Additional space is also required for content updates and logs.

Table 9: Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to the system drive

Client type	Requirements
Standard	**With the program data folder located on the system drive:** • 395 MB* **With the program data folder located on an alternate drive:** • System drive: 180 MB • Alternate installation drive: 350 MB
Embedded / VDI	**With the program data folder located on the system drive:** • 245 MB* **With the program data folder located on an alternate drive:** • System drive: 180 MB • Alternate installation drive: 200 MB
Dark network	**With the program data folder located on the system drive:** • 545 MB* **With the program data folder located on an alternate drive:** • System drive: 180 MB • Alternate installation drive: 500 MB

* An additional 135 MB is required during installation.

Table 10: Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to an alternate drive

Client type	Requirements
Standard	**With the program data folder located on the system drive:** • System drive: 380 MB • Alternate installation drive: 15 MB* **With the program data folder located on an alternate drive:**** • System drive: 30 MB • Program data drive: 350 MB • Alternate installation drive: 150 MB
Embedded / VDI	**With the program data folder located on the system drive:** • System drive: 230 MB • Alternate installation drive: 15 MB* **With the program data folder located on an alternate drive:**** • System drive: 30 MB • Program data drive: 200 MB • Alternate installation drive: 150 MB
Dark network	**With the program data folder located on the system drive:** • System drive: 530 MB • Alternate installation drive: 15 MB* **With the program data folder located on an alternate drive:**** • System drive: 30 MB • Program data drive: 500 MB • Alternate installation drive: 150 MB

* An additional 135 MB is required during installation.

** If the program data folder is the same as the alternate installation drive, add 15 MB to the program data drive for your total. However, the installer still needs the full 150 MB to be available on the alternate installation drive during installation.

Table 11: Symantec Endpoint Protection client for Windows Embedded system requirements

Component	Requirements
Processor	1 GHz Intel Pentium
Physical RAM	256 MB **Note:** This figure is for an installation of the Symantec Endpoint Protection embedded client. If you also implement additional features from an integrated solution such as EDR, additional physical RAM is needed.
Hard drive	The Symantec Endpoint Protection Embedded / VDI client requires the following available hard disk space: • Installed to the system drive: 245 MB • Installed to an alternate drive: 230 MB on system drive, and 15 MB on the alternate drive An additional 135 MB is needed during installation. These figures assume that the program data folder is on the system drive. For more detailed information, or for the requirements of the other client types, see the Symantec Endpoint Protection client for Windows system requirements.

Component	Requirements
Embedded operating system	• Windows Embedded Standard 7 (32-bit and 64-bit) • Windows Embedded POSReady 7 (32-bit and 64-bit) • Windows Embedded Enterprise 7 (32-bit and 64-bit) • Windows Embedded 8 Standard (32-bit and 64-bit) • Windows Embedded 8.1 Industry Pro (32-bit and 64-bit) • Windows Embedded 8.1 Industry Enterprise (32-bit and 64-bit) • Windows Embedded 8.1 Pro (32-bit and 64-bit)
Required minimum components	• Filter Manager (FltMgr.sys) • Performance Data Helper (pdh.dll) • Windows Installer Service
Templates	• Application Compatibility (Default) • Digital Signage • Industrial Automation • IE, Media Player, RDP • Set Top Box • Thin Client The Minimum Configuration template is not supported. The Enhanced Write Filter (EWF) and the Unified Write Filter (UWF) are not supported. The recommended write filter is the File Based Write Filter (FBWF) installed along with the Registry Filter.

Table 12: Symantec Endpoint Protection client for Mac system requirements

Component	Requirements
Processor	64-Bit Intel Core 2 Duo or later
Physical RAM	2 GB of RAM
Hard drive	500 MB of available hard disk space for the installation
Display	800 x 600
Operating system	• macOS 10.13 • macOS 10.14 • macOS 10.15 to 10.15.5 macOS 10.14.5 and later support the kext notarization requirements. See Endpoint Protection 14.2 RU1 and kext notarization for macOS 10.14.5. For a list of supported operating systems for previous releases, see: Mac compatibility with the Endpoint Protection client

Table 13: 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 - 7U7, 8; 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, 7U4 • Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U8, 8-8U2 • 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, 18.04 (as of 14.3); 32-bit and 64-bit For a list of supported operating system kernels for previous releases, see List of Linux Distributions and Kernels with Precompiled Auto-Protect Drivers/Modules for Symantec Endpoint Protection for Linux 14.x.
Graphical desktop environments	You can use the following graphical desktop environments to view the Symantec Endpoint Protection for Linux client: • KDE • Gnome • Unity

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 libnsl.i686`
	– For Debian-based distributions: `sudo apt-get install ia32-libs`
	– For Ubuntu-based distributions:
	`sudo dpkg --add-architecture i386`
	`sudo apt-get update`
	`sudo apt-get install gcc-multilib libx11-6:i386`
	• net-tools or iproute2
	Symantec Endpoint Protection uses one of these two tools, depending on what is already installed on the computer.
	• 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
	• To display the system tray icon, the following requirements must be met on a client device:
	– **libdbus**
	Install using one of the following commands:
	Ubuntu 18 or higher: `apt-get install libdbus-1-dev:i386`
	RHEL 8 or higher: `yum install dbus-devel.i686`
	– **AppIndicator**
	System tray functionality is dependent on **libappindicator** support.
	https://doc.qt.io/qt-5/qsystemtrayicon.html
	On a target Ubuntu 18 or higher device, you must enable **AppIndicator** extension at the following path:
	Activities > *Software* > *Add-ons* > *Shell Extensions* > *KStatusNotifierItem/AppIndicatorSupport*
	On a target RHEL 8 or higher device, you must install **AppIndicator** extension to the following location:
	Applications > *System Tools* > *Software* > *Add-ons* > *Shell Extensions* > *KStatusNotifierItem/AppIndicatorSupport*

Release notes and system requirements for all versions of Symantec Endpoint Protection

Supported and unsupported upgrade paths to the latest version of Symantec Endpoint Protection 14.x

Generally, for Symantec Endpoint Protection versions earlier than the latest version, every version on the list before it is supported. However, you should confirm by referring to the release notes for your specific version.

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

Supported upgrade paths

- Symantec Endpoint Protection Manager 14.x upgrades seamlessly over 12.1.x, except where support has been dropped, such as: Windows Server 2003, desktop operating systems, and 32-bit operating systems, as well as some versions of SQL Server.
- The Symantec Endpoint Protection 14.x client upgrades seamlessly over all previous 12.1 and 11 client versions installed on supported operating systems. The exception is the Mac client earlier than 12.1.4, which you must upgrade to 12.1.4 or later, or uninstall it.

Symantec Endpoint Protection 14 Migration Considerations

Symantec Endpoint Protection Manager and Windows client

The following versions of Symantec Endpoint Protection Manager and Symantec Endpoint Protection Windows client can upgrade directly to the current version:

- 11.x and Small Business Edition 12.0 (Symantec Endpoint Protection clients only, for supported operating systems)
- 12.1.x, up to 12.1.6 MP10
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU1 MP2
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

Mac client

The following versions of Symantec Endpoint Protection client for Mac can upgrade directly to the current version:

- 12.1.4 - 12.1.6 MP9

The Mac client did not update for version 12.1.6 MP10.
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

NOTE

The Symantec Endpoint Protection client for Mac was not updated for 14.0.1 MP2.

Linux client

The following versions of Symantec Endpoint Protection client for Linux can upgrade directly to current version:

- 12.1.x, up to 12.1.6 MP9
  The Linux client did not update for version 12.1.6 MP10.
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU1 MP2
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

Symantec AntiVirus for Linux 1.0.14 is the only version that you can migrate directly to Symantec Endpoint Protection. You must first uninstall all other versions of Symantec AntiVirus for Linux. You cannot migrate a managed client to an unmanaged client.

Unsupported upgrade paths

You cannot migrate to Symantec Endpoint Protection from all Symantec products. You must uninstall the following products before you install the Symantec Endpoint Protection client.

- Symantec AntiVirus and Symantec Client Security, which are not supported.
- All Symantec Norton ™ products
- Symantec Endpoint Protection for Windows XP Embedded 5.1
- Any Symantec Endpoint Protection for Mac client earlier than 12.1.4. Or you can upgrade it to 12.1.4 or later.

Notes:

- Any Symantec Endpoint Protection client migration for version earlier than 12.1.x is not supported.
- You cannot upgrade Symantec Endpoint Protection Manager 11.0.x or Symantec Endpoint Protection Manager Small Business Edition 12.0.x directly to any version of Symantec Endpoint Protection Manager 14. You must first uninstall these versions or perform an upgrade to 12.1.x before an upgrade to the latest release of 14.x.
- You cannot upgrade Symantec Endpoint Protection Manager 12.1.6 MP7 to version 14 because the database schema version in 12.1.6 MP7 is later than in 14. Instead, you must upgrade 12.1.6 MP7 to 14 MP1 or later.
- 14.0.x dropped support for Windows XP, Server 2003, and any Windows Embedded operating system that is based on Windows XP. Symantec Endpoint Protection Manager 14.2 RU1 can manage these computers as legacy 12.1.x clients, although 12.1.x clients are EOL. For these clients, you may want to use a Symantec product that still supports these legacy operating systems, such as Data Center Security (DCS).
- Upgrading from 14 MP1 (14.0.2332.0100) to 14 MP1 Refresh Build (14.0.2349.0100) is not supported.
- Downgrade paths are not supported. For example, if you want to migrate from Symantec Endpoint Protection 14.2.1.1 to 12.1.6 MP10, you must first uninstall Symantec Endpoint Protection 14.2.1.1

If you have a build number but you are not sure how it translates to release version, see:

- Release versions, notes, new fixes, and system requirements for Endpoint Security and all versions of Endpoint Protection
- About Endpoint Protection release types and versions

Where to get more information

The following table displays the websites where you can get best practices, troubleshooting information, and other resources to help you use the product.

Table 14: Endpoint Protection website information

Types of information	Website link
Trial versions	Contact your account representative.
Manuals and documentation updates	• Product guides for the latest release (English) • Product guides for the latest release (other languages) • Product guides for all versions of Symantec Endpoint Protection 14.x (English)
Technical Support	Endpoint Protection Technical Support Includes knowledge base articles, product release details, updates and patches, and contact options for support.
Threat information and updates	Symantec Security Center
Training	Education Services Access the training courses, the eLibrary, and more.
Symantec Connect forums	Endpoint Protection


Symantec
A Division of Broadcom