Symantec™ Endpoint Protection 14.3 RU3 Release Notes

Updated: September 17, 2021

Table of Contents

Copyright statement

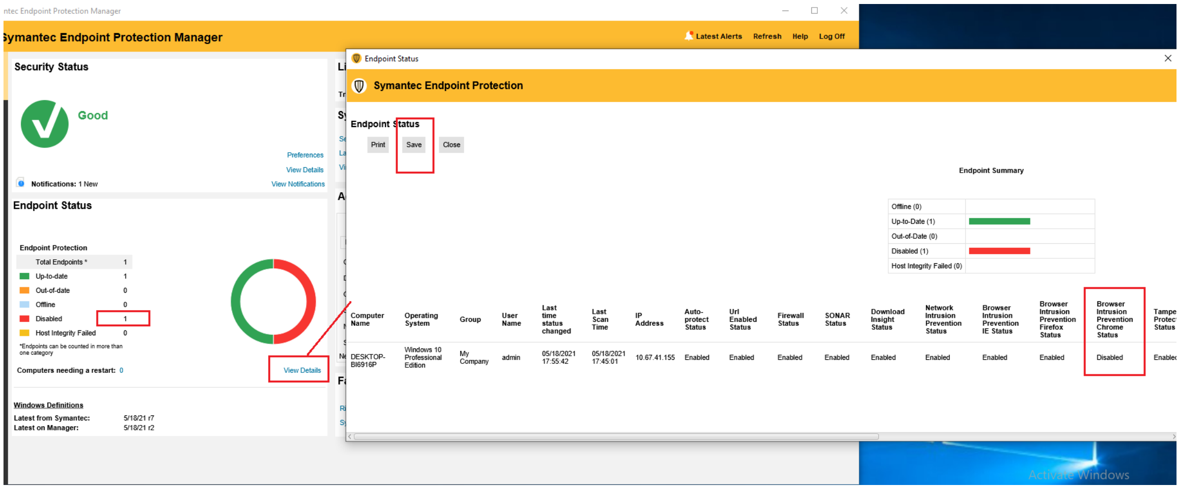
Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use 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.

What's new for Symantec Endpoint Protection 14.3 RU3?

This section describes the new features in this release.

Protection features

- Enhanced protection against living-off-the-land tools. For more information, see: How Symantec Endpoint Protection protects against ransomware threats and living-off-the land tactics
- Improved protection for threats on Linux using Machine Learning and cloud analytics. To leverage this capability, in the **Virus and Spyware Protection policy,** click **Linux Settings** > **Global Scan Options**.
- Symantec can now release new detection capabilities via Auto-Protect much faster.
- Enhanced reporting of the browser extension status in the Symantec Endpoint Protection Manager:
  - The **Clients** page > **Clients** tab > **Protection technology** view displays whether the browser extensions are enabled or disabled. Select the client and click **Edit Properties**> **Clients** tab. The **Browser IE Enabled Status**, **Browser FF Enabled Status**, and **Browser Chrome Enabled Status** fields show either the **Enabled**, **Disabled**, or **Not reporting** status. **Browser Extension Definitions** show the version number for the definitions.
  - On the **Home** page, under **Endpoint Status**, select the clients that have the **Disabled** status, and click **Details**. In the report, view the browser extensions that are enabled or disabled.



Endpoint Protection

Total Endpoints *	1
🟩 Up-to-date	1
🟧 Out-of-date	0
🟦 Offline	0
🟥 Disabled	1
🟨 Host Integrity Failed	0

*Endpoints can be counted in more than one category

Computers needing a restart: 0

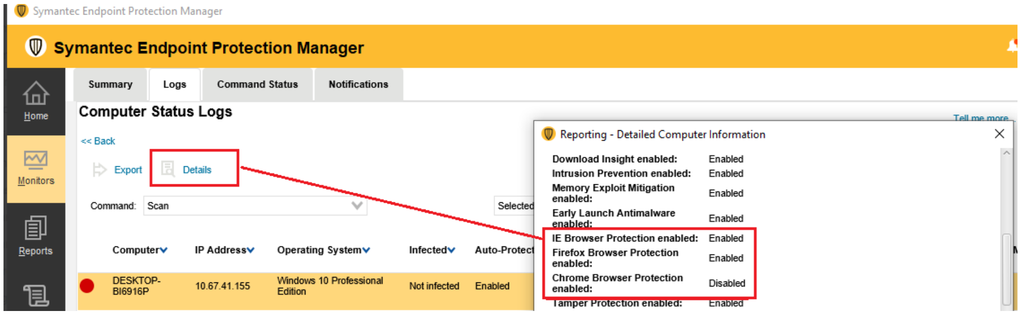
Windows Definitions

Latest from Symantec: 5/18/21 r7
Latest on Manager: 5/18/21 r2

Offline (0)	
Up-to-Date (1)	🟩
Out-of-Date (0)	
Disabled (1)	🟥
Host Integrity Failed (0)	

Computer Name	Operating System	Group	User Name	Last time status changed	Last Scan Time	IP Address	Auto-protect Status	Url Enabled Status	Firewall Status	SONAR Status	Download Insight Status	Network Intrusion Prevention Status	Browser Intrusion Prevention IE Status	Browser Intrusion Prevention Firefox Status	Browser Intrusion Prevention Chrome Status	Tampe Protec Status
DESKTOP-BI6916P	Windows 10 Professional Edition	My Company	admin	05/18/2021 17:55:42	05/18/2021 17:45:01	10.67.41.155	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled	Enablec

  - Enhanced reporting of clients with the browser extension disabled. On the **Home** page, under **Favorite Reports**, the **Symantec Endpoint Protection Weekly Status** report displays which clients have the extensions that are enabled or disabled.
  - The **Protection Content Versions** quick report shows when the Chrome browser extension definitions were last updated. Click the **Reports** > **Quick Reports** > **Computer Status** report type > **Protection Content Versions** report, and click **Create Report**. Click the **Security Status Summary** report to see how many clients have the browser extensions that are disabled or malfunctioning.
  - The Computer Status log displays columns for **IE Browser Protection Enabled**, **Firefox Browser Protection Enabled**, and **Chrome Browser Protection Enabled**. On the **Monitors** page, click **Logs** > **Computer Status** log > **View Log**. On the **Logs** tab, click **Details** for the revision number for **Browser Extensions Definitions**. Use this information to make sure the browser extension content is downloaded to the client.



Computer Status Logs

Command: Scan

	Computer	IP Address	Operating System	Infected	Auto-Protect
●	DESKTOP-BI6916P	10.67.41.155	Windows 10 Professional Edition	Not infected	Enabled

Reporting - Detailed Computer Information

Download Insight enabled:	Enabled
Intrusion Prevention enabled:	Enabled
Memory Exploit Mitigation enabled:	Enabled
Early Launch Antimalware enabled:	Enabled
IE Browser Protection enabled:	Enabled
Firefox Browser Protection enabled:	Enabled
Chrome Browser Protection enabled:	Disabled
Tamper Protection enabled:	Enabled

– The client System log displays an event every time that the Chrome browser extension is enabled, disabled, installed, uninstalled, or removed.

Integrating browser extensions with Symantec Endpoint Protection to protect against malicious websites

Symantec Endpoint Protection Manager updates

- Symantec Endpoint Protection Manager now supports Windows Server 2022.
- Flexibility to control the automatic upgrade of clients using the Client Upgrade policy. The policy supports location-awareness so that you can target subgroups. The policy also allows the upgrade to occur any day of the week, be distributed over multiple days, and to be retried if it did not start as scheduled.

  Upgrading client software with the Client Upgrade policy

  Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager
- If the client detects it has outdated content, Windows clients provide continuous protection by checking for updates at a regular interval. If the definitions are missing, the client logs an event once every 30 minutes. Legacy clients attempt remediation a set number of times before stopping for the day and logging an error. You control this setting with the Virus and Spyware Protection policy > **Miscellaneous** > **Notifications** tab > **Remediation attempts before a warning appears in Symantec Endpoint Protection** option.
- The following third-party components were upgraded or added: AjaxSwing, Apache HTTP Server, libcurl, libxml2, OpenJDK, OpenSSL, and PHP.

Client and platform updates

Client and platform updates

Windows Client:

- The Windows client is supported on Windows Server 2022 and Windows 10 Embedded. Version 14.3 RU3 has been tested and is compatible with all Windows 11 and Windows 11 Embedded pre-release versions.
- If a Symantec Endpoint Protection Manager domain is enrolled in the cloud, a troubleshooting page appears with the names of the policies that the cloud console manages. To access this page, click **Help** > **Troubleshooting** > **Hybrid Management**.
- **Debug log**: When you enable the client `debug.log` in the **Help** > **Troubleshooting** > **Debug Logs** panel, you also enable the `cve.log` . You do not need to restart the client or run the following commands for any changes in the debug log to take effect: `smc -stop` or `smc -start` . The client debug logs help troubleshoot client-to-Symantec Endpoint Protection Manger communication problems and client functionality problems. You find the communication logs (`cve.log` , `cve-actions.log`) in **C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Logs**.

  Advanced debug log options in SymDiag for Endpoint Protection clients

  Configuring Endpoint Protection Communication Module Logging in 14.2 and later

Mac Client:

> **NOTE**
> The Symantec Endpoint Protection client for Mac 14.3 RU3 release is planned for October 2021.

- Added support for macOS 12.
- The size of the Mac client installer has been reduced to 100 MB.
- The number of **'At Risk'** alarms has been reduced and optimized.
- To enhance performance, multiple scans can no longer run simultaneously. If a scan is running, other scans are queued.
- As of version 14.3 RU3, the Mac client installer does not allow installing an earlier version of the client.

Linux Agent:

- You can install the Linux Agent off-line using the installation package from a local repository.
- The Linux Agent command-line tool (sav) has been enhanced with options for showing versions, running LiveUpdate, and starting and stopping a scan. For more information, see:
  Managing your Linux Agent using the command line tool (sav)
- You can upgrade and uninstall the Linux Agent without restarting it.
- Linux now supports TCP for SEPM-managed computers.
- Defect fixes.

- Removed the warning for the **Use Symantec servers when private servers are not available** option in **Clients** page > **Clients** tab > **External Communications**. 12.1.5 clients are no longer supported.

Documentation changes

- The Symantec Endpoint Protection Manager APIs are in a PDF file on the following location:
  ENDPOINT SECURITY REST API DOCUMENTATION

What's new in all releases of Symantec Endpoint Protection

Known issues and workarounds for Symantec Endpoint Protection (SEP)

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

NOTE

The Issue column displays the version number when the issue appears. For example, [14.3 RU1] means that the issue applies to version 14.3 RU1 and later. When these issues are fixed, they appear in the fix-it notes. See:

Versions, system requirements, release dates, notes, and fixes for Symantec Endpoint Protection and Endpoint Security

Upgrade issues

Issue	Description and solution
The following error message appears: "Symantec Endpoint Protection version 14.3 RU2 for Win64bit is the latest package. You cannot delete it." [14.3 RU2]	You cannot delete the Client Install Package when packages from multiple builds appear in the Symantec Endpoint Protection Manager. As of 14.3 RU2, LiveUpdate can download multiple client installation packages with a different build number, which appear in the **Admin** page > **Install Packages** > **Client Install Package** table. [SEP-72531]
AutoUpgrade fails if you use the 14.3 RU2 **Upgrade to English if currently installed language is unsupported** option to upgrade clients with an unsupported language to English. [14.3 RU2]	This issue occurs for clients that you manually upgraded from a supported to an unsupported language in 14.3 RU1 MP1 and earlier, such as upgrading a Czech client to a Japanese client on a Japanese operating system. And then used to the **Upgrade to English if currently installed language is unsupported** option to upgrade the unsupported language to English in 14.3 RU2. [SEP-72490] This issue is caused because the client language uses the language of the supported operating system (in this case, Japanese). AutoUpgrade expects to use the supported language and not English. To work around this issue, try the AutoUpgrade again and turn off the **Upgrade to English if currently installed language is unsupported** option.
When exporting a client installation package from a 14.3 RU2 Symantec Endpoint Protection Manager (SEPM), the following warning message appears: "The client installation package does not have content." [14.3 RU2]	This issue occurs when communication between the Symantec Endpoint Protection Manager and the console being used to export the package is disrupted. See: "The client installation package does not have content." warning when exporting an installation package from the Endpoint Protection Manager
An error appears when importing the most recent client installation packages into an older version of Symantec Endpoint Protection Manager. [14.3 RU2]	Symantec Endpoint Protection 14.3 RU2 clients cannot be managed by a 14.3 RU1 MP1 or earlier Symantec Endpoint Protection Manager. [SEP-72292]

Issue	Description and solution
After upgrading a Symantec Endpoint Protection Manager to 14.3 RU2, php-cgi.exe crashes with an error in the event viewer [14.3 RU2]	This issue occurs with the 17.4.1.1 version of the Microsoft ODBC Driver for SQL Server. [SEP-70385] To work around this issue, download and install the 17.7.2 version of the Microsoft ODBC Driver for SQL Server on Windows: https://docs.microsoft.com/en-us/sql/connect/odbc/windows/release-notes-odbc-sql-server-windows?view=sql-server-ver15 For more information, see: php-cgi.exe crash occurs on Endpoint Protection Manager after upgrading to 14.3 RU2
After upgrading to Symantec Endpoint Protection Manager 14.3 RU2, "The client computer has been renamed" notifications may appear [14.3 RU2]	After upgrading from an older version of Symantec Endpoint Protection Manager to 14.3 RU2, administrators may start receiving "The client computer has been renamed" notifications. This issue is applicable only to Mac clients. See: "The client computer has been renamed" notifications may appear after upgrading to Symantec Endpoint Protection Manager 14.3 RU2
A Symantec Endpoint Protection Manager in a dark network downloads old Client Intrusion Detection System (CIDS) content to new clients because LiveUpdate does not run during an upgrade [14.3 RU1]	When a 14.3 RU1 Symantec Endpoint Protection Manager cannot access either the Internet or a LiveUpdate Administrator (LUA) server, it keeps old, incompatible content in its cache. This old content is normally delivered to the new clients. To update the content in the management server's cache, you manually download certified virus definitions and CIDS .jdb files. [SEP-69125] To make sure that the new clients do not get old content, manually install a CIDS .jdb file on SEPM before you install new clients or upgrade old clients. See: Download .jdb files to update definitions for Endpoint Protection Manager
Cannot log on to Symantec Endpoint Protection Manager (SEPM) when the network interface card is disabled [14.3 RU1]	If after you install Symantec Endpoint Protection Manager, you cannot log on to the console and the following error message appears: `Unexpected server error` This issue may occur if the computer's network interface card is disabled when you installed the SEPM, which keeps the server certificate from being generated. [SEP-67040] To find out if SEPM was installed with a disabled network interface card, look at the server certificate. See: Unexpected server error at SEPM login if it was installed on a server without an enabled NIC
When you uninstall SEPM and use the option to remove the default database and leave the SQL Server Express instance, the following error appears: "`An error occurred while trying to connect to the database server`" [14.3 RU1]	If you uninstall the Symantec Endpoint Protection Manager and select the **Remove only the DB and leave the SQL Server Express instance installed with SEPM** option, you may see the following error: "`An error occurred while trying to connect to the database server`." This issue occurs after you add the credentials for the default user DBA and may be related to user privileges. [SEP-68670] To work around this issue, perform the uninstallation by running the SEPM setup.exe file and clicking the **Remove only the DB and leave the SQL Server Express instance installed with SEPM** option during uninstallation.
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. For more information, see: SQL upgrade from 2017 to 2019 fails with FIPS mode enabled

Issue	Description and solution
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.

Symantec Endpoint Protection Manager issues

Issue	Description and solution
Endpoint Protection (SEP) 14.2 RU1 MP1 and earlier clients do not honor the **Upgrade Schedule** settings in a Client Upgrade Policy [14.3 RU3]	For more information, see: Endpoint Protection 14.3 RU1 MP1 and older clients not following Client Upgrade Policy [SEP-72814]
Some EDR events do not appear on the client [14.3 RU1]	The Symantec Endpoint Protection client must run Windows 10 build 14393 or later to collect Symantec EDR Event Tracing for Windows (ETW) events. [SEP-67175]
The Network Traffic Redirection (Web and Cloud Access Protection) feature has some limitations [14.3 RU1]	• The Symantec Web Security Service is delivered on IPv4 and not IPv6. [SEP-68700] • The tunnel redirection method: – Runs on Windows 10 x64 version 1703 and later (Semi-Annual Servicing Channel) only. This method does not support any other Windows operating systems or the Mac client. [SEP-67927] – Does not support HVCI-enabled Windows 10 64-bit devices. [SEP-67648] – Redirects outbound traffic from the Symantec Endpoint Protection client to the WSS before it gets evaluated by either the client's firewall or the URL reputation rules. Instead, that traffic is evaluated against the WSS firewall and the URL rules. For example, if a SEP client firewall rule blocks google.com and a WSS rule allows google.com, the client allows users to access google.com. Inbound local traffic to the client is still processed by the Symantec Endpoint Protection firewall. [SEP-67488] – The WSS Captive Portal is not available for the tunnel method, and the client ignores the challenge credentials. In a future release, SAML authentication in the WSS agent will replace the Captive Portal, and will be available in the Symantec Endpoint Protection client. – If a client computer connects to the WSS using the tunnel method and hosts virtual machines, each guest user needs to install the SSL certificate provided in the WSS portal. – Traffic for local network like your home directory or Active Directory authentication is not redirected. – Is not compatible with the Microsoft DirectAccess VPN. The tunnel method is currently considered an early adopter release feature.
Duplicate client enrollment entries after the upgrade from 14.2.x to 14.3 MP1 and later [14.3 RU1]	Upgrading the Symantec Endpoint Protection clients from 14.2.x to 14.3 MP1 and later creates duplicate agent enrollment entries for these clients on the **Clients** page in Symantec Endpoint Protection Manager. There is no functional impact and you can continue working with the new entries for 14.3 RU1 clients. Symantec Endpoint Protection Manager will remove older agent entries.

Issue	Description and solution
Allow URLs in Symantec Endpoint Security if you use the hybrid management option, proxy servers or a perimeter firewall [14.3]	With Broadcom’s 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. You allow the URLs in either fully cloud-managed or hybrid-managed agents, allow thein your proxy server and/or perimeter firewall. See: • URLs that allow SEP and SES to connect to Symantec servers • 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]	In 14.3 and later, 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."
"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.

Windows, Mac, and Linux client issues

Issue	Description and solution
Unexpected server error when logging into Endpoint Protection Manager and clients are no longer communicating after a system time change [14.3 RU3]	If you set the system clock back to a previous date and/or time, the following error may occur: • After you log on to the Symantec Endpoint Protection Manager, an Unexpected Server Error appears. • The clients do not communicate with SEPM, which reports a 503 error. [SEP-74510] To work around this issue: • Manually restart the SEPM services. • Wait until the date/time on the system passes the original time on the system before you set it back.
Endpoint Protection 14.3 RU3 Web and Cloud Access Protection log reports Windows 10 Operating System on Windows 11 [14.3 RU3]	When the client user views the SEP client Web and Cloud Access Protection log, the log shows the operating system as Windows 10 when when the client is installed on a Windows 11 device. On the client console, click **Web and Cloud Access Protection** > **Options** > **View Logs**.)
Microsoft Edge browser and the Google Chrome browser are not able to launch after the **Validate image dependency integrity** mitigation technique is applied to the Windows 10 or 11 operating system. [14.3 RU3]	One of the mitigation techniques that Microsoft Edge uses to protect the Windows operating system is the **Validate image dependency integrity** technique. For Windows 10 or 11 computers that run the Symantec Endpoint Protection clients versions 14.2 RU2 MP1 or later, if this option is enabled, both Microsoft Edge and the Google Chrome web browsers do not launch. [SEP-75086] To ensure that Microsoft Edge launches, disable the **Validate image dependency integrity** technique. For more information on mitigation techniques for Microsoft Edge, see: Customize exploit protection See also: Microsoft Edge and Google Chrome do not open if "Validate image dependence integrity" mitigation technique is applied and SEP 14.2 RU2 MP1 or later is installed
You must restart the rebootless Windows client to obtain latest EDR events [14.3 RU3]	To make additional ETW events available in 14,3 RU3, you must restart the Symantec Endpoint Protection client. You must restart the client in the following situations: [SEP-73327] • If EDR is enabled and you update the client to RU3. • 14.3 RU3 is already installed and you enable or disable EDR. You must restart the client to enable or disable the newly added events. See: A restart may be required to begin seeing some ETW events with EDR and SEP 14.3 RU3
Scan Engine fails to initialize after the Linux client upgrade. [14.3 RU3]	Scan Engine fails to initialize after upgrading Symantec Endpoint Protection client for Linux to version 14.3 RU3. **Workaround:** 1. Update the LiveUpdate Server with latest content that would have SEF 1.7.6. 2. Uninstall Linux client 14.3 RU3 that is exhibiting the "Scan Engine initialization failure" error. 3. Reinstall Linux client 14.3 RU3.
`auditd` daemon will be enabled after the Linux client installation. [14.3 RU3]	Symantec Endpoint Protection client for Linux installer enables `auditd` daemon after the agent installation even if `auditd` daemon was disabled before the installation.
For collecting the network forensic information (EDR), `netstat` package is required on the Linux client. [14.3 RU3]	If the `netstat` package is missing on the Linux client, the forensic information is collected for all other types of events except for network events.

Issue	Description and solution
Possible connection issues on Mac devices. [14.3 RU2]	• After upgrading the Mac agent using AutoUpgrade and restarting the device, the agent might fail to connect to the network. **Workaround:** Rerun the agent installation package. • After being in standby mode, a Mac device might lose its network connection with the following error: "Your connection was interrupted. A network change was detected." **Workarounds:** – If you use a docking station, renew the IP addresses manually at **System Preferences > Network**. – Unplug the docking station from your Mac device for a few seconds and then plug it in again.
Rosetta may block the Mac agent installation on Apple Silicon (M1) devices with the following error: "This version of Symantec Agent for Mac is not supported on Apple M1 chip." [14.3 RU2]	For more information, see: KB 222282
Downloading and installing Mac agent using the Web link that was generated in Symantec Endpoint Protection Manager may fail. [14.3 RU2]	If an admin invites users to install the Mac agent 14.3 RU2 using the **Web Link and Email** option in Symantec Endpoint Protection Manager and the users download the package using this link in the Safari browser, the installation of the Mac agent may fail with the following error: "The application Symantec Endpoint Protection Installer can't be opened" **Workarounds:** • After downloading the file, go to the **Downloads** folder, execute the following command, and then run the installation again: `chmod +x ./Symantec\ Endpoint\ Protection/Symantec\ Endpoint\ Protection\ Installer.app/Contents/MacOS/Symantec\ Endpoint\ Protection\ Installer` • Open Safari browser's **Preferences** and on the **General** tab, uncheck the option **Open "safe" files after downloading**. Then download the installer package, and run the installation.
If you automatically upgrade a client with an unsupported language to English, the client continues to display the date settings for definitions in English [14.3 RU1 and later]	To work around this issue, uninstall the legacy client and manually install a new English client installation package. In addition, a fix is expected for clients that are upgraded automatically. [SEP-72481]
The standalone Symantec WSS Agent blocks the Symantec Endpoint Protection client installation if you install SEP on the same computer as the WSS Agent	The Network Traffic Redirection (NTR) component uses the same files as the standalone Symantec WSS Agent (WSSA). NTR is installed by default in both Symantec Endpoint Protection and the Symantec Endpoint Security cloud console. If the NTR feature is installed on an endpoint, WSSA cannot be installed. Similarly, if WSSA is installed, the NTR feature does not install. You can remove the Network Traffic Redirection feature from existing endpoints without having to uninstall the whole client by using one of the following methods: • In Symantec Endpoint Protection Manager, create a Client Install Feature Set that does not include NTR and apply it to the endpoints. See: Add or remove features to existing Endpoint Protection clients • The following command line option uses the client installation file to remove NTR: `setup.exe /s /v" REMOVE=NTR /qn"`
Upgrade installation package that is used for clean installation installs default feature set. [14.3 RU1 MP1 and earlier]	If you create an upgrade installation package with **Maintain existing client features when updating** option checked, and use this package to do a clean installation, the default feature set will be installed on your client device. If you want to install a custom feature set, you must create a separate installation package for the clean installation.

Issue	Description and solution
Unsupported upgrade path creates duplicate devices in cloud console. [14.3 RU1]	Upgrading your macOS from 10.15 to 11.0 before upgrading the Symantec Agent for Mac from 14.2/14.3 to 14.3 RU1 creates duplicate devices in cloud console. To avoid duplicates, you must upgrade the client before upgrading the operating system (i.e. upgrade the Symantec Agent for Mac from 14.2/14.3 to 14.3 RU1 and then upgrade macOS from 10.15 to 11.0.).
Incorrect messages in the Symantec Agent for Linux installer log. [14.3 RU1]	In some cases, the agent installer logs incorrect messages related to a non-matching driver version or a required reboot. These messages do not affect the functionality of the agent.
On a SuSe Linux device, zypper removes the SEP Linux client packages while removing the 'at' package. [14.3 RU1]	On a SuSe Linux device, the command 'zypper remove at' removes the SEP Linux client packages because the 'at' package is added as a required dependent package and the zypper commands automatically attempt to remove the SEP client packages 'sdcss-kmod' and 'sdcss-sepagent' as the packages with unused dependencies. **Workaround:** To remove the 'at' package, run the following command: rpm -e --nodeps at
Upgrade issue on macOS 10.15 and later [14.3 MP1]	On macOS 10.15 and later, the **Install Symantec Endpoint Protection to Remote Computers** feature in the Client Deployment Wizard fails to upgrade the Symantec Endpoint Protection client from older versions to version 14.3 MP1. **Workaround:** Use **Symantec Endpoint Protection Manager Auto Upgrade** to perform the Symantec Endpoint Protection client upgrade on macOS 10.15 and later.
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.

For resolved issues, see:

- New fixes and components for Symantec Endpoint Protection 14.3 RU3
- New fixes and components for Symantec Endpoint Protection 14.3 RU1 MP1
- New fixes and components for Symantec Endpoint Protection 14.3 RU1
- New fixes and components for Symantec Endpoint Protection 14.3 MP1
- New fixes and components for Symantec Endpoint Protection 14.3

Documentation

You can find documentation on 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**.

To find a PDF file, release notes, or the Symantec Endpoint Protection Manager database schema, go to the Related Documents page. In the future, Broadcom will be adding legacy PDF files and translated PDF files.

System requirements for Symantec Endpoint Protection (SEP) 14.3 RU3

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 1: 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 • Windows Server 2022 **Note:** Desktop operating systems are not supported. **Note:** Windows Server Core edition is not supported on 14.2x and earlier.
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 Chromium Based Browser (14.3 and later) • Microsoft Edge Note: The 32-bit version Windows 10 does not support web console access on the Edge browser. • Microsoft Internet Explorer 11 (14.2.x and earlier) • Mozilla Firefox 5.x through 83 • Google Chrome 87

Component	Requirements
Database	The Symantec Endpoint Protection Manager includes a default database: • Microsoft SQL Server Express 2014 (for Windows Server 2008 R2) • Microsoft SQL Server Express 2017 • Sybase embedded database (14.3 MP.x and earlier only) 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 SP1, SP2 • SQL Server 2017 RTM • SQL Server 2019 RTM (14.3 and later) **Note:** SQL Server databases that are hosted on Amazon RDS are supported. (14.0.1 MP2 and later). **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. See: **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. • Microsoft Visual C++ 2017 Redistributable Package (x64/x86) Note that the required version of Visual C++ is automatically installed during the installation of Symantec Endpoint Protection Manager

Table 2: 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 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

Component	Requirements
Hard drive when installing to an alternate drive	With 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
Other	An enabled network interface card

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 3: 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) (14.3 and later) • Windows 10 20H2 (Windows 10 version 2009) (14.3 and later) • Windows 10 21H1 (as of 14.3 RU1) • Version 14.3 RU3 has been tested and is compatible with all Windows 11 pre-release versions.
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) • Windows Server, version 2004 • Windows Server, version 20H2 (14.3 RU1) • Windows Server 2022 (as of 14.3 RU3) For a list of supported operating systems for previous releases, see: • Windows compatibility with the Endpoint Protection client • Endpoint Protection support for Windows 10 updates and Windows Server 2016 / Server 2019
Browser Intrusion Prevention	Browser Intrusion Prevention support is based on the version of the Client Intrusion Detection System (CIDS) engine. See: See Supported browsers for Browser Intrusion Prevention in Endpoint Protection

Table 4: 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 5: 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 6: 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 7: 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) • Windows Embedded 10 • Version 14.3 RU3 has been tested and is compatible with all Windows 11 Embedded pre-release versions.
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 8: Symantec Endpoint Protection client for Mac system requirements

Component	Requirements
Processor/Chip	64-Bit Intel Core 2 Duo or later Apple M1 chip (as of 14.3 RU2)
Physical RAM	2 GB of RAM
Hard drive	1 GB of available hard disk space for the installation
Display	800 x 600
Operating system	• macOS 10.15 to 10.15.7 • macOS 11 (Big Sur) For a list of supported operating systems for previous releases, see: Mac compatibility with the Endpoint Protection client

Table 9: Symantec Endpoint Protection client for Linux system requirements

Component	Requirements
Hardware	• Intel Pentium 4 (2 GHz) or later processor • 1 GB of free RAM (4 GB of RAM is recommended) • 2 GB available disk space if `/var`, `/opt`, and `/tmp` share the same filesystem or volume • 500 MB available disk space in each `/var`, `/opt`, and `/tmp` if on different volumes
Operating systems	Supported operating systems as of version 14.3 RU1: • Amazon Linux 2 • CentOS 6, 7, 8 • Debian 9, 10 (14.3 RU2 and later) • 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 more information, and for lists of supported minor Linux OS versions, see: Supported kernels of Symantec Linux Agent Supported operating systems for version 14.3 MP1 and earlier: • 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
Other environmental requirements (14.3 RU1 and later)	• OpenSSL 1.0.2k-fips or later

Component	Requirements

Other environmental requirements (14.3 MP1 and earlier)	• 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.
	• 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
	• 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`

Graphical desktop environments	You can use the following graphical desktop environments to view the Symantec Endpoint Protection for Linux client: • KDE • Gnome • Unity Symantec Agent for Linux 14.3 RU1 does not have a graphical user interface.

More information

Release versions, notes, new fixes, and system requirements for Endpoint Security and all versions of 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. See:

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

Supported upgrade paths

- Symantec Endpoint Protection Manager version 12.1.6 MP10 and later with the embedded database upgrades seamlessly to the Microsoft SQL Server Express database, version 14.3 RU1 MP1. Upgrades from 12.1.6 MP9 and earlier to 14.3 RU1 MP1 are blocked.
- 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 client versions installed on supported operating systems. See:

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
- 14.3, 14.3 MP1
- 14.3 RU1, 14.3 RU1 MP1, 14.3 RU2

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 RU1 MP2

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

- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1
- 14.3 RU1, 14.3 RU1 MP1 (available June 2021), 14.3 RU2

Linux client

> **NOTE**
> 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 of the new client. Old configurations are not retained.

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
- 14.3, 14.3 MP1
- 14.3 RU1, 14.3 RU1 MP1, 14.3 RU2

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.

Additional information

- 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.
- If you have a build number but you are not sure how it translates to release version, see:
  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 10: Endpoint Protection website information

Types of information	Website link
Trial versions	Contact your account representative.
Manuals and documentation updates	Related Documents page For other languages, click the **English** drop-down menu.
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