Symantec™ Endpoint Protection 14.3 RU1 Release Notes

Updated: December 18, 2020

Table of Contents

Copyright statement

What's new for Symantec Endpoint Protection 14.3 RU1?

This section describes the new features in this release.

Protection Features

- Includes the new Symantec Mac Agent and the Symantec Linux Agent that can be installed and managed from either the on-premises Symantec Endpoint Protection Manager or the Integrated Cyber Defense Manager cloud console.
  Installing the Symantec Endpoint Protection client for Mac
  Installing the Symantec Agent for Linux 14.3 RU1
- Prevents new and unknown threats on the macOS by monitoring file behaviors in real time. The new Mac Agent includes these behavioral protection capabilities. Behavioral protection, or SONAR, uses artificial intelligence and advanced machine learning for zero-day protection to effectively stop new threats.
  Managing SONAR
- Blocks untrusted non-portable executable (PE) files such as PDF files and scripts that are not yet identified as a threat. In the Exceptions policy, click **Windows Exceptions** > **File Access**.
- Prevents web threats based on the reputation score of a web page. The Intrusion Prevention policy includes URL reputation filtering, which blocks web pages with reputation scores below a specific threshold. Reputation scores range from -10 (bad) to +10 (good). The **Enable URL Reputation** option is enabled by default.
- You can force Symantec Endpoint Protection to learn an application based on the application's hash value. In the Exceptions policy, click **Windows Exceptions** > **Application** > **Add an Application by Fingerprint**.
- Protects endpoints and users from web-based attacks on malicious sites using the Network Traffic Redirection feature. Network Traffic Redirection redirects all network traffic (any port) or just web-based traffic (ports 80 and 443) to the Symantec Web Security Service, which allows or blocks network traffic and SaaS application access based on the enterprise policy. The Network Traffic Redirection policy has a new redirection method called the tunnel method. The tunnel method automatically redirects all Internet traffic to the Symantec WSS, where the traffic is allowed or blocked based on the Symantec Web Security Service policies. The tunnel method is considered a beta feature. You should perform thorough testing with your applications against your WSS policies. Broadcom has a beta website that offers a testing guide and a place to leave feedback on your experience. Log on to the following website using your Broadcom credentials: Validate.broadcom.com.
  Configuring Network Traffic Redirection
- The Integrations policy was renamed to the Network Traffic Redirection policy.
- Provides support for MITRE-enriched events in Symantec EDR. Leverage the MITRE ATT&CK framework to provide context into what is happening in your environment.
- Provides support for the following Symantec EDR events, which expose more visibility into the endpoints:
  - AMSI events provide visibility of threat actor methods that can evade traditional command-line interrogation methods.
  - ETW events provide visibility into events happening on managed Windows endpoints.
- Includes the ability to run both the Windows Defender and Symantec Endpoint Protection on the same computer. The Auto-Protect scan runs after Windows Defender and can detect any threats that Windows Defender misses. The **Coexist with Windows Defender** option ensures that Auto-Protect runs in case Microsoft Defender is disabled. To disable the option, click the Virus and Spyware Protection policy > **Miscellaneous** > **Miscellaneous** tab.
- Attack chain mitigation is now supported for hybrid-managed clients.

Symantec Endpoint Protection Manager

- The embedded database was updated to the Microsoft SQL Express database. The SQL Server Express database stores policies and security events more efficiently than the default embedded database and is installed automatically with the Symantec Endpoint Protection Manager.

Best practices for upgrading from the embedded database to the Microsoft SQL Server Express database

- During the installation or upgrade of the Symantec Endpoint Protection Manager, the Management Server Configuration wizard:
  - Automatically installs LiveUpdate content.
  - Provides an option to use TLS certificate for secure communication between SQL Server and the Symantec Endpoint Protection Manager.
- LiveUpdate uses a new engine in Symantec Endpoint Protection Manager, which is optimized to run on the cloud console. The new engine no longer supports the FTP method or LAN method to specify an internal LiveUpdate server to download content to the Symantec Endpoint Protection Manager.

  Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager
- The **Automatically uninstall existing third-party security software** option that was not available in 14.3 MP1 is available again in 14.3 RU1 with an updated version. This option is used to uninstall third-party security software. To access this option, click **Admin** page > **Packages** > **Client Install Settings**.

  Third-party security software removal in Endpoint Protection 14

  Third-party security software removal in Endpoint Protection 14.3 RU1
- The Client Deployment Wizard that is used to deploy client packages must have its credentials verified and able to connect to the Symantec Endpoint Protection Manager. If the verification process fails, the client deployment process stops to keep Active Directory user accounts from being locked.

  Installing Symantec Endpoint Protection clients with Remote Push
- The Computer Status logs and reports now lets you select a range for the **Client version** and **IPS version** fields. The **Product version** filter was renamed to **Client version**.
- The **Disable the notification tray icon** option is available for clients that run on a terminal server and that cause high CPU usage and memory usage. You can now disable the notification area icon, also known as the system tray icon, to prevent multiple instances of user session processes (like SmcGui.exe and ccSvcHost.exe) from running. For clients that run on a terminal server, the **Disable the notification area icon** option overrides the registry key setting in HKLM\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\LaunchSMCGui. In lieu of manually changing this key, it is now managed via policy. As a best practice, move clients that are on a terminal server in the same group before you upgrade. For clients that do not run on a terminal server, keep this setting disabled. This option takes place only after the client smc service is restarted. You enable this option on the **Clients** > **Policies** tab > **General** > **General Settings** tab.
- Updated the whitelist and blacklist mode to reflect the allow and block functionality. On the **Clients** page > **Policies** tab > **System Lockdown** dialog box, the application file lists changed from **Whitelist Mode** and **Blacklist Mode** to **Allow Mode** and **Deny Mode**.
- On the **Admin** page > **Servers** tab > **Configure External Logging** > **General** tab, the **Master Logging Server** option changed to **Primary Logging Server**.
- The **System** log type > **Administrative** log and the **Audit** log lists the computer name.
- Client firewall logs are collected so that you get fewer notifications on the cloud console.
- Replaced the Oracle Java SE with the OpenJDK.
- Updated the third-party components JQuery to a newer version.

Client and platform updates

- The Windows client supports Windows 10 20H2 (Windows 10 version 2009).
- Moved the legacy Mac client installation packages to the AdditionalPackages folder.

Features Removed

- The **Risk severity** and **Risk Distribution by Severity** options were removed from notifications and reports.
- The **CASMA** tab and **Analyze** command were removed, as this functionality was deprecated in 14.3.
- The Mac client no longer supports macOS 10.13 or 10.14.x.
- You can no longer view exclusions in the registry. For 14.3 RU1 and earlier, to view exclusions, see: Verify if an Endpoint Client has Automatically Excluded an Application or Directory

Documentation

The Symantec Endpoint Protection Manager Help is now online and located at: Symantec Endpoint Protection Installation and Administration Guide

Database schema

The database schema has the following changes.

Table	Column change
ALERTS	Added the ENRICHED_DATA column.
AGENT_BEHAVIOR_LOG1 AGENT_BEHAVIOR_LOG2 AGENT_PACKET_LOG_1 AGENT_PACKET_LOG_2 AGENT_SECURITY_LOG_1 AGENT_SECURITY_LOG_2 AGENT_SYSTEM_LOG_1 AGENT_SYSTEM_LOG_2 AGENT_TRAFFIC_LOG_1 AGENT_TRAFFIC_LOG_2 BASIC_METADATA COMMAND COMPUTER_APPLICATION ENFORCER_CLIENT_LOG_1 ENFORCER_CLIENT_LOG_2 ENFORCER_SYSTEM_LOG_1 ENFORCER_SYSTEM_LOG_2 ENFORCER_TRAFFIC_LOG_1 ENFORCER_TRAFFIC_LOG_2 IDENTITY_MAP LAN_DEVICE_DETECTED LAN_DEVICE_EXCLUDED LEGACY_AGENT LOCAL_METADATA LOG_CONFIG REPORTS SEM_APPLICATION SEM_CLIENT SEM_COMPUTER SEM_JOB SEM_SVA_CLIENT SEM_SVA_COMPUTER SERVER_ADMIN_LOG_1 SERVER_ADMIN_LOG_2 SERVER_CLIENT_LOG_1 SERVER_CLIENT_LOG_2	Removed the following columns from each table: RESERVED_INT1 RESERVED_INT2 RESERVED_BIGINT1 RESERVED_BIGINT2 RESERVED_CHAR1 RESERVED_CHAR2 RESERVED_VARCHAR1 RESERVED_BINARY

Table	Column change
SERVER_ENFORCER_LOG_1 SERVER_ENFORCER_LOG_2 SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 SERVER_SYSTEM_LOG_1 SERVER_SYSTEM_LOG_2 SYSTEM_STATE V_AGENT_BEHAVIOR_LOG V_AGENT_PACKET_LOG V_AGENT_SECURITY_LOG V_AGENT_SYSTEM_LOG V_AGENT_TRAFFIC_LOG V_DOMAINS V_ENFORCER_CLIENT_LOG V_ENFORCER_SYSTEM_LOG V_ENFORCER_TRAFFIC_LOG V_GROUPS V_LAN_DEVICE_DETECTED V_LAN_DEVICE_EXCLUDED V_SEM_COMPUTER V_SERVER_ADMIN_LOG V_SERVER_CLIENT_LOG V_SERVER_ENFORCER_LOG V_SERVER_SYSTEM_LOG V_SERVERS	(Continued)
BINARY_FILE SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 V_SERVER_POLICY_LOG	• The CONTENT column changed its type from 'image' to ‘varbinary’ • Added an FILESTREAM_ID indexed column • Added a FILESTREAM_ID index • Removed the following columns: – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
INVENTORYREPORT	Added the following columns: • PRODUCTVERSIONFROM • PRODUCTVERSIONTO • IDS_VERSIONFROM • IDS_VERSIONTO

Table	Column change
SEM_AGENT	• Added the NTR_MESSAGE column. • Removed the following columns: – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
SEM_AGENT_VERSION	Added the following columns: • VERSION • FORMATTED_VERSION • REFRESH_USN • AGENT_VERSION_FORMAT_REFRESH • VERSION1 • VERSION2 • VERSION3 • VERSION4
SEM_SVA	Removed the following columns: • RESERVED_INT1 • RESERVED_INT2 • RESERVED_BIGINT1 • RESERVED_BIGINT2 • RESERVED_CHAR1 • RESERVED_CHAR2 • RESERVED_VARCHAR1
V_ALERTS	Added the ENRICHED_DATA column.

What's new in all releases of Symantec Endpoint Protection

Known issues and workarounds for Symantec Endpoint Protection

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

Table 1: Upgrade issues

Issue	Description and solution
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. 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. 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. 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.

Table 2: Symantec Endpoint Protection Manager issues

Issue	Description and solution
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 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 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 a beta feature.
Duplicate agent 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 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]	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.

Table 3: Windows, Mac, and Linux client issues

Issue	Description and solution
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

Issue	Description and solution
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.

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 RU1

New fixes and components for Symantec Endpoint Protection 14.3 MP1

New fixes and components for Symantec Endpoint Protection 14.3

System requirements for Symantec Endpoint Protection (SEP) 14.3 RU1

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 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 RTM, 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 (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 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 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

Component	Requirements
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 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) (14.3 and later) • Windows 10 20H2 (Windows 10 version 2009) (as of 14.3 RU1)
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) 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

Component	Requirements
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	1 GB of available hard disk space for the installation
Display	800 x 600
Operating system	• macOS 10.15 to 10.15.7 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 • 500 MB of free RAM (4 GB of RAM is recommended) • 2 GB available disk space if `/var`, `/opt`, and `/tmp` share the same filesystem 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 • 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 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.
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.

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.
	• OpenSSL 1.0.2k-fips or later
	• 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`

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.

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. Upgrades from 12.1.6 MP9 and earlier to 14.3 RU1 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 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
- 14.3, 14.3 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 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

  NOTE

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

Linux client

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

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.t
- 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

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.
- 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 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