Symantec™ Endpoint Protection 12.1.6 MP10 Release Notes

Symantec Endpoint Protection Release Notes

Product version: 12.1.6 MP10

Documentation version: 1

This document was last updated on: April 16, 2018

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information

- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Release notes

This document includes the following topics:

About this document

This document contains information for Symantec Endpoint Protection.

Review this document before you install the product or before you call Technical Support. The release notes describe known issues and their workarounds that are not included in the standard documentation or online Help.

See “Known issues and workarounds” on page 7.

See “System requirements for Symantec Endpoint Protection” on page 10.

What's New in Symantec Endpoint Protection 12.1.6 MP10

This version of Symantec Endpoint Protection includes new features, changes, or improvements in the following areas:

- Customer defects

- Third-party component updates

What's new in all releases of Symantec Endpoint Protection 12.1.x

See "Known issues and workarounds" on page 7.

Known issues and workarounds

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

- See "Installation information" on page 7.
- See "Symantec Endpoint Protection Manager information" on page 7.
- See "Documentation and help information" on page 8.

You can view a list of resolved issues for this release at the following location:

New fixes and component versions in Symantec Endpoint Protection 12.1.6 MP10

Installation information

This section includes information about installing the product.

Installation of or upgrade to Symantec Endpoint Protection Manager 12.1.6 MP10 is blocked on Windows XP / Server 2003

Due to a PHP version upgrade, Symantec Endpoint Protection Manager is no longer supported on Windows XP / Server 2003. PHP 5.6.27 provides security improvements over previous versions. No workaround is available. Instead, you must either upgrade the computer or move Symantec Endpoint Protection Manager to a new computer that runs a supported Windows operating system.

For information on moving Symantec Endpoint Protection Manager 12.1.x to a new server, see Move Endpoint Protection Manager to another server without breaking client communications or losing data.

Symantec Endpoint Protection Manager information

This section contains information about Symantec Endpoint Protection Manager.

HTTPS communications fail to Symantec Endpoint Protection clients installed on Windows XP / Server 2003

Client communications to Windows XP / Server 2003 computers fail with HTTPS communications enabled in Symantec Endpoint Protection 12.1.6 MP10. This failure occurs because of a cipher mismatch.

Use the procedure at the following page to work around this issue:

HTTPS communications fail to Endpoint Protection clients installed on Windows XP / Server 2003

Web console access does not work with Internet Explorer 8-10

Due to a JRE version upgrade, Symantec Endpoint Protection Manager no longer supports Internet Explorer 8, 9, or 10 as of 12.1.6 MP9. Web console access to Symantec Endpoint Protection Manager 12.1.6 MP10 fails when you use these versions of Internet Explorer. Instead, use Internet Explorer 11, or an alternate supported browser.

See “Symantec Endpoint Protection Manager system requirements” on page 11.

Remote Java Console access to Symantec Endpoint Protection Manager fails with FIPS enabled

In a FIPS-compliant environment, access to Symantec Endpoint Protection Manager 12.1.6 MP10 fails with the error: "Failed to validate certificate. The application will not be executed." This error results from an incompatibility between Crypto-J and JRE 8. To work around this issue, access Symantec Endpoint Protection Manager using the web console.

Remote Java Console access to Endpoint Protection Manager fails with FIPS enabled

Firewall displays in Symantec Endpoint Protection Manager web console as Fire...

When you log on to Symantec Endpoint Protection Manager through the web console, in the **Policies** tab, **Firewall** incorrectly displays as **Fire...**. This issue is a cosmetic one. A fix is planned for a future release.

Windows LiveUpdate displays English text for localized versions of Symantec Endpoint Protection Manager

Symantec Endpoint Protection Manager includes Windows LiveUpdate, which downloads content to make it available to managed clients. In localized versions of Symantec Endpoint Protection Manager, you notice that Windows LiveUpdate displays English-only dialogs.

This behavior is currently as expected. Windows LiveUpdate is planned to be localized in future versions of Symantec Endpoint Protection.

Documentation and help information

This section contains changes or additions to the documentation and context-sensitive help.

Help erroneously indicates that alerts do not generate for all SONAR action types

The Help topic SONAR: SONAR incorrectly suggests that for **When detection found**, an alert does not appear when the action is Log only. An alert appears for all action types when a SONAR detection is made, not just for Quarantine or Remove. The corrected text for **When detection found** is as follows:

Configures notifications to alert the user when SONAR makes a detection.

Help does not include information about maximum bandwidth for client downloads from a Group Update Provider (GUP)

In Symantec Endpoint Protection Manager, the context-sensitive help topic **Group Update Provider** does not include descriptive information for the setting **Maximum bandwidth allowed for client downloads from Group Update Provider**. The description is as follows:

Maximum bandwidth allowed for client downloads from Group Update Provider: Use this option if you want to set up a Group Update Provider to service multiple sites that have a few clients only. This feature helps you to minimize the bandwidth for the sites that have low connectivity and where you want to avoid content storms when you deliver a full set of content definitions.

Corrections and additions to the database schema reference for 12.1.6

The following items are missing from the database schema reference for Symantec Endpoint Protection 12.1.6, or are incorrect.

Table 1-1 Database schema reference updates for 12.1.6

Item	Update
Agent Behavior Logs entries indicate the incorrect unit of measurement	Agent Behavior Logs schema entries that are associated with application control violations list the file sizes in megabytes (MB). This file size should instead read bytes, both in the database and in the client logs. Affected are the following: ■ AGENT_BEHAVIOR_LOG_1 ■ AGENT_BEHAVIOR_LOG_2 ■ BEHAVIOR_REPORT

Table 1-1 Database schema reference updates for 12.1.6 *(continued)*

Item	Update
Values missing for the ACTUALACTION table	The ACTUALACTION table erroneously omits the following values: ■ 24 - RepairFailedPowerEraser A Power Eraser scan is recommended. Symantec Endpoint Protection cannot remove or clean the threat. Symantec Endpoint Protection can only block the threat. ■ 25 - RepairFailedPowerEraser2 A Power Eraser scan is recommended. Symantec Endpoint Protection cannot remove or clean the threat. Symantec Endpoint Protection cannot confirm that it blocked the threat. ■ 100 - IDS block ■ 101 - Firewall violation ■ 102 - Allowed by user ■ 200 - Attachment stripped
Values for Agent Behavior logs for column DESCRIPTION	For the table AGENT_BEHAVIOR_LOG_1, the DESCRIPTION column has a 256-character limit. Therefore, actual values from the client may be longer than the ones that are displayed in Symantec Endpoint Protection Manager logs or reports. Check on the client to confirm.

For the 12.1.6 database schema reference, see: Symantec Endpoint Protection 12.1.6 database schema.

System requirements for Symantec Endpoint Protection

In general, the system requirements for Symantec Endpoint Protection Manager and the Symantec Endpoint Protection clients are the same as those of the operating systems on which they are supported.

For the most current system requirements, see:

System requirements for Symantec Endpoint Protection 12.1.6 MP10

- See "Symantec Endpoint Protection Manager system requirements" on page 11.
- See "Symantec Endpoint Protection client for Windows system requirements" on page 13.
- See "Symantec Endpoint Protection client for Windows Embedded system requirements" on page 15.
- See "Symantec Endpoint Protection client for Mac system requirements" on page 16.
- See "Symantec Endpoint Protection client for Linux system requirements" on page 17.

See "Supported virtual installations and virtualization products" on page 18.

Symantec Endpoint Protection Manager system requirements

Note: This Symantec Endpoint Protection Manager version manages 11.0.x and 12.0.x clients, regardless of the client operating system. However, support for Symantec Endpoint Protection 11.0.x and 12.0.x ended January 5, 2015.

Table 1-2 Symantec Endpoint Protection Manager system requirements

Component	Requirements
Processor	Intel Pentium Dual-Core or equivalent minimum **Note:** Intel Itanium IA-64 processors are not supported.
Physical RAM	2 GB RAM available minimum; 4 GB or more available recommended **Note:** Your Symantec Endpoint Protection Manager server might require additional RAM depending on the RAM requirements of other applications that are already installed.
Hard drive	16 GB available minimum (100 GB recommended) for the management server 40 GB available minimum (200 GB recommended) for the management server and a locally installed database
Display	1024 x 768 or larger
Operating system (desktop)	■ Windows 7 (32-bit, 64-bit; RTM and SP1; all editions except Starter and Home) ■ Windows 8 (32-bit, 64-bit) ■ Windows 8.1 (32-bit, 64-bit) ■ Windows 8.1 update for April, 2014 (32-bit, 64-bit) ■ Windows 8.1 update for August, 2014 (32-bit, 64-bit) **Note:** Windows 7 allows only 20 concurrent connections. Installing Symantec Endpoint Protection Manager on Windows 7 is only recommended for smaller environments. See Best practices for installing Endpoint Protection Manager on Windows 7 or XP for configuration recommendations.

Table 1-2 Symantec Endpoint Protection Manager system requirements *(continued)*

Component	Requirements
Operating system (server)	■ Windows Server 2008 (32-bit, 64-bit; R2, RTM, SP1 and SP2) ■ Windows Small Business Server 2008 (64-bit) ■ Windows Essential Business Server 2008 (64-bit) ■ Windows Small Business Server 2011 (64-bit) ■ 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 **Note:** Windows Server Core edition is not supported. Windows Server Core does not include Internet Explorer, which Symantec Endpoint Protection Manager requires to work.
Web browser	The following browsers are supported for web console access to Symantec Endpoint Protection Manager and for viewing the Symantec Endpoint Protection Manager Help: ■ Microsoft Internet Explorer 11 See "Web console access does not work with Internet Explorer 8-10" on page 8. ■ Mozilla Firefox 5.x through 59.x ■ Google Chrome 65.x
Database	The Symantec Endpoint Protection Manager includes an embedded database. You may instead choose to use a database from one of the following versions of Microsoft SQL Server: ■ SQL Server 2005, SP4 ■ SQL Server 2008, RTM - SP4 ■ SQL Server 2008 R2, RTM - SP3 ■ SQL Server 2012, RTM - SP3 ■ SQL Server 2014, RTM - SP2 ■ SQL Server 2016 **Note:** The SQL Server Express Edition database is not supported. **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. For more information: TLS 1.2 support for Microsoft SQL Server

Note: 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.

See "Supported virtual installations and virtualization products" on page 18.

Symantec Endpoint Protection client for Windows system requirements

Table 1-3 Symantec Endpoint Protection client for Windows system requirements

Component	Requirements
Processor	■ 32-bit processor: 1 GHz Intel Pentium III 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.
Physical RAM	512 MB (1 GB recommended) or higher if required by the operating system
Hard drive	1.8 GB of available hard disk space for the installation; additional space is required for content and logs **Note:** Space requirements are based on NTFS file systems.
Display	800 x 600 or larger

Table 1-3 Symantec Endpoint Protection client for Windows system requirements *(continued)*

Component	Requirements
Operating system (desktop)	■ Windows XP Home or Professional (32-bit, SP3; 64-bit, SP2) ■ Windows XP Embedded (SP3) ■ Windows Vista (32-bit, 64-bit) ■ 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, Industry Enterprise (32-bit and 64-bit) ■ Windows 10 (32-bit, 64-bit) ■ Windows 10 November Update (2015) (32-bit, 64-bit) ■ Windows 10 Anniversary Update (2016) (32-bit, 64-bit) (basic compatibility) ■ Windows 10 Creators Update (2017) (32-bit, 64-bit) (basic compatibility) ■ Windows 10 Fall Creators Update (2017) (32-bit, 64-bit) (basic compatibility) ■ Windows 10 Spring Creators Update (2018) (32-bit, 64-bit) (basic compatibility) See Endpoint Protection support for Windows 10 updates and Windows Server 2016 for important details on basic compatibility. See “Symantec Endpoint Protection client for Windows Embedded system requirements” on page 15.
Operating system (server)	■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later) ■ Windows Small Business Server 2003 (32-bit) ■ Windows Server 2008 (32-bit, 64-bit; R2, SP1, and SP2) ■ Windows Small Business Server 2008 (64-bit) ■ Windows Essential Business Server 2008 (64-bit) ■ Windows Small Business Server 2011 (64-bit) ■ 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 (Basic compatibility) See Endpoint Protection support for Windows 10 updates and Windows Server 2016 for important details on basic compatibility.

Table 1-3 Symantec Endpoint Protection client for Windows system requirements *(continued)*

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.

See "Supported virtual installations and virtualization products" on page 18.

Symantec Endpoint Protection client for Windows Embedded system requirements

Table 1-4 Symantec Endpoint Protection client for Windows Embedded system requirements

Component	Requirements
Processor	1 GHz Intel Pentium
Physical RAM	256 MB
Hard drive	450 MB of available hard disk space
Embedded operating system	■ Windows Embedded Standard (WES) 2009 (32-bit, SP3) ■ Windows Embedded POSReady 2009 (32-bit, SP3) ■ Windows Embedded Point of Service (WEPOS) (32-bit, SP3) ■ 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 ■ FBA: Driver Signing (applies only to XP-based Embedded) ■ WinLogon (applies only to XP-based Embedded)

Table 1-4 Symantec Endpoint Protection client for Windows Embedded system requirements *(continued)*

Component	Requirements
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.

See Symantec Endpoint Protection support for Windows Embedded.

See "Supported virtual installations and virtualization products" on page 18.

Symantec Endpoint Protection client for Mac system requirements

Table 1-5 Symantec Endpoint Protection client for Mac system requirements

Component	Requirements
Processor	64-Bit Intel Core 2 Duo or later
Physical RAM	2 GB of RAM
Hard drive	500 MB of available hard disk space for the installation
Display	800 x 600
Operating system	Mac OS X 10.8, 10.9, 10.10, 10.11, and macOS 10.12 **Note:** 12.1.6 MP10 is not supported on macOS 10.13.

Symantec Endpoint Protection client for Linux system requirements

Table 1-6 Symantec Endpoint Protection client for Linux system requirements

Component	Requirements
Hardware	■ Intel Pentium 4 (2 GHz) or later processor ■ 1 GB of RAM ■ 7 GB of available hard disk space
Operating systems	■ Amazon Linux ■ CentOS 6U4, 6U5, 6U6, 6U9, 7, 7U1, 7U2, 7U3; 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 ■ Novell Open Enterprise Server (OES) 2 SP2 and 2 SP3 running SUSE Linux Enterprise Server (SLES) 10 SP3; 32-bit and 64-bit ■ Novell Open Enterprise Server (OES) 11 and 11 SP1 running SUSE Linux Enterprise Server (SLES) 11 SP1 and SP2; 64-bit ■ Oracle Linux (OEL) 5U8, 5U9, 6U2, 6U4, 6U5; 64-bit ■ Red Hat Enterprise Linux Server (RHEL) 5U7 - 5U11, 6U2 - 6U9, 7 - 7U3; 32-bit and 64-bit ■ SUSE Linux Enterprise Server (SLES) 10 SP3, 10 SP4, 11 SP1 - 11 SP3; 32-bit and 64-bit ■ SUSE Linux Enterprise Desktop (SLED) 10 SP3, 10 SP4, 11 SP1 - 11 SP3; 32-bit and 64-bit ■ Ubuntu 11.10, 12.04, 12.04.02, 14.04, 16.04; 32-bit and 64-bit For a list of supported operating system kernels, see Supported Linux kernels for Symantec Endpoint Protection.
Graphical desktop environments	You can use the following graphical desktop environments to view the Symantec Endpoint Protection for Linux client: ■ KDE ■ Gnome ■ Unity

Table 1-6 Symantec Endpoint Protection client for Linux system requirements *(continued)*

Component	Requirements
Other environmental requirements	■ Oracle Java 1.5 or later; Java 7 or later recommended This installation requires superuser privileges. ■ Unlimited Strength Java Cryptography Extension (JCE) You must install the Unlimited Strength Java Cryptography Extension policy files to match your version of Java. This installation requires superuser privileges. You can download the installation files under **Additional Resources** from the following Oracle website: http://www.oracle.com/technetwork/java/javase/downloads/ ■ 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` ■ For Debian-based distributions: `sudo apt-get install ia32-libs` ■ For Ubuntu-based distributions: `sudo apt-get install libx11-6:i386 libgcc1:i386 libc6:i386` ■ net-tools To install Symantec Endpoint Protection on Red Hat Enterprise Linux Server (RHEL) 7.1 or later, you must first install net-tools. ■ XFS file systems that contain inode64 attributes are not supported. ■ 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

See "Supported virtual installations and virtualization products" on page 18.

Supported virtual installations and virtualization products

You can install Symantec Endpoint Protection on supported operating systems that run in virtual environments. Install Symantec Endpoint Protection on the guest operating system, and not the host.

The following virtualization products support the Symantec Endpoint Protection Manager, console, and embedded database components, and Symantec Endpoint Protection client software for Windows and Linux:

- Windows Azure
- Amazon WorkSpaces
- VMware WS 5.0 (workstation) or later
- VMware GSX 3.2 (enterprise) or later
- VMware ESX 2.5 (workstation) or later
- VMware ESXi 4.1 - 5.5
- VMware ESXi 6.0
- VMware ESXi 6.0 Update 1
- VMware ESXi 6.0 Update 2
- Microsoft Virtual Server 2005
- Microsoft Enterprise Desktop Virtualization (MED-V), which includes Windows XP mode
- Windows Server 2008 Hyper-V
- Windows Server 2012 Hyper-V
- Windows Server 2012 R2 Hyper-V
- Citrix XenServer 5.6 or later
- Virtual Box, supplied by Oracle

Supported upgrade paths to Symantec Endpoint Protection

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 12.1.6 MP10:

- 11.0.x and Small Business Edition 12.0.x
  See Supported upgrade and migration paths to Symantec Endpoint Protection 12.1.x.
- 12.1 RTM (12.1.671.4971)
- 12.1.1 (12.1.1000.157)
- 12.1.1 MP1 (12.1.1101.401)

- 12.1.2 (12.1.2015.2015)
- 12.1.2 MP1 (12.1.2100.2093)
- 12.1.3 (12.1.3001.165)
- 12.1.4 (12.1.4013.4013)
- 12.1.4a (12.1.4023.4080)
- 12.1.4 MP1 (12.1.4100.4126)
- 12.1.4 MP1a (12.1.4104.4130)
- 12.1.4 MP1b (12.1.4112.4156b)
- 12.1.5 (12.1.5337.5000)
- 12.1.6 (12.1.6168.6000)
- 12.1.6 MP1 (12.1.6306.6100)
- 12.1.6 MP1a (12.1.6318.6100)
- 12.1.6 MP2 (12.1.6465.6200
- 12.1.6 MP3 (12.1.6608.6300)
- 12.1.6 MP4 (12.1.6867.6400)
- 12.1.6 MP5 (12.1.7004.6500)
- 12.1.6 MP6 (12.1.7061.6600)
- 12.1.6 MP7 (12.1.7166.6700)
- 12.1.6 MP8 (12.1.7266.6800)
- 12.1.6 MP9 (12.1.7369.6900)
- 12.1.6 MP9a (12.1.7385.6900)

Mac client

The following versions of Symantec Endpoint Protection client for Mac can upgrade directly to 12.1.6 MP10:

- 12.1 RTM (12.1.671.4971)
- 12.1.1 (12.1.1000.157)
- 12.1.2 (12.1.2015.2015)
- 12.1.4 (12.1.4013.4013)
- 12.1.5 (12.1.5337.5000)
- 12.1.6 (12.1.6168.6000)

- 12.1.6 MP2 (12.1.6465.6200)
- 12.1.6 MP4 (12.1.6867.6400)
- 12.1.6 MP6 (12.1.7061.6600)
- 12.1.6 MP8 (12.1.7266.6800)
- 12.1.6 MP9 (12.1.7369.6900)

Note: The Symantec Endpoint Protection client for Mac was not updated for 12.1.3, 12.1.6 MP1 / MP1a, 12.1.6 MP3, 12.1.6 MP5, and 12.1.6 MP7.

Linux client

The following versions of Symantec Endpoint Protection client for Linux can upgrade directly to 12.1.6 MP10:

- 12.1.5 (12.1.5337.5000)
- 12.1.6 (12.1.6168.6000)
- 12.1.6 MP3 (12.1.6608.6300)
- 12.1.6 MP4 (12.1.6867.6400)
- 12.1.6 MP5 (12.1.7004.6500)
- 12.1.6 MP6 (12.1.7061.6600)
- 12.1.6 MP7 (12.1.7166.6700)
- 12.1.6 MP8 (12.1.7266.6800)
- 12.1.6 MP9 (12.1.7369.6900)

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 12.1.6 MP10 client:

- The unsupported Symantec products Symantec AntiVirus and Symantec Client Security
- All Symantec Norton™ products
- Symantec Endpoint Protection for Windows XP Embedded 5.1

Downgrade paths are not supported. For example, if you want to migrate from Symantec Endpoint Protection 14.0.1 MP1 to 12.1.6 MP10, you must first uninstall Symantec Endpoint Protection 14.0.1 MP1.

Supported upgrades to Windows 10 with the Symantec Endpoint Protection client installed

You can upgrade to Windows 10 with the Symantec Endpoint Protection client installed, as follows:

- Upgrade to Windows 10 with 12.1.6 MP1 or later installed.
- Upgrade to Windows 10 Anniversary Update or Creators Update with 12.1.6 MP5 or later installed.
- Upgrade to Windows 10 Fall Creators Update with 12.1.6 MP9 or later installed.

Before you upgrade Windows, you must ensure that Virus and Spyware Protection definitions are from July 27, 2015, or later. Definitions as of this date include an update to the Eraser engine (115.1.1.10) that is required for Windows 10 compatibility.

You must uninstall any Symantec Endpoint Protection client versions earlier than those versions already specified. The operating system upgrade stops if it detects an earlier version of Symantec Endpoint Protection.

The following operating system upgrade paths are supported with the appropriate compatible client version installed:

- Windows 8.1 to Windows 10
- Windows 8 to Windows 10
- Windows 7 to Windows 10

Note: Windows 7 does not include Early Launch Antimalware (ELAM). Therefore, the Symantec Endpoint Protection ELAM component is not enabled, and does not enable after you upgrade to Windows 10 with Symantec Endpoint Protection installed. Your protection level is the same as it was with Windows 7.

To allow the Symantec Endpoint Protection client to recognize ELAM and enable the Symantec Endpoint Protection ELAM component, you must uninstall and reinstall Symantec Endpoint Protection. You can also upgrade from 12.1.6 MP1 to the latest version of Symantec Endpoint Protection to recognize the ELAM component. Repairing the client installation does not enable the ELAM component.

Where to get more information

Table 1-7 displays the websites where you can get best practices, troubleshooting information, and other resources to help you use the product.

Table 1-7 Symantec website information

Types of information	Website link
Trial versions	Trialware (14.x)
Manuals and documentation updates	**English:** ■ Symantec Product Documentation ■ Product guides for all versions of Symantec Endpoint Protection 12.1.x ■ Product guides for all versions of Symantec Endpoint Protection 14 **Other languages:** ■ Brazilian Portuguese ■ Chinese (simplified) ■ Chinese (traditional) ■ French ■ German ■ Italian ■ Japanese ■ Korean ■ Spanish *Czech, Polish, and Russian files are on the English page.
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	■ Symantec Education Services Access the training courses, the eLibrary, and more.
Symantec Connect forums	Endpoint Protection