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
- What’s new in Symantec Endpoint Protection 14.0.1 MP1
- Known issues and workarounds
- System requirements for Symantec Endpoint Protection
- Supported upgrade paths to Symantec Endpoint Protection
- Where to get more information

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 9.

See “System requirements for Symantec Endpoint Protection” on page 15.

What's new in Symantec Endpoint Protection 14.0.1 MP1

- Cloud portal protection features
- Protection features
- Management server features
Symantec Endpoint Protection provides application isolation. Application isolation protects users from malicious macros in Microsoft Office, malicious PDF files, and browser plug-ins with vulnerabilities. Application Isolation protects applications from overwrites by other applications if both the applications use same resource. For example, infected tab of a browser may end up sharing the same memory with the other tab. One infected tab may infect the tabs on other browsers.

Symantec Endpoint Protection Hardening provides a set of policies that you can use to isolate applications so that they operate in a protected environment.

Read more about application isolation in the Hardening Technical white paper: Delivering Zero-Day Defenses with Symantec Endpoint Protection.

Protection features

WSS Traffic Redirection
Symantec Endpoint Protection provides web security to remote users by connecting the client to Web Security Services (WSS) when a route through a corporate network is not possible or practical. WSS Traffic Redirection (WTR) directs traffic from the endpoint to WSS/CASB Services, eliminating the need to install a separate client. You deploy them once and manage them centrally, which lowers the cost of management and eliminates conflict between the agents. This functionality allows Symantec Endpoint Protection to rapidly enable connectivity to cloud services with minimal interruption to users.

Ability to test new engine content and definitions before they are released
Symantec Endpoint Protection contains several content engines that carry out parts of its functionality. Symantec provides a special server that lets you download and test the engine content before you roll out the content to your production environment. Engine updates are released to the EAS for 2 weeks before its phased release on the public LiveUpdate server. Symantec provides the engine updates using your regular LiveUpdate configuration.

You can find the option Use a Symantec LiveUpdate early release server in the LiveUpdate Settings policy.

Testing engine updates before they release on Windows clients

Option to lock engine version
The LiveUpdate Content policy now has the option to revert to an older version of the engine but continue to receive the latest content that corresponds with that engine. In the
LiveUpdate Content policy under **Windows Settings**, click **Security Definitions > Select an engine version > Edit**. Clients that are locked to a specific engine version only receive LiveUpdate content that corresponds to that engine version.

**Reverting to an older version of the Symantec Endpoint Protection security updates**

**Management server features**

- On the Symantec Endpoint Protection Manager Home page banner, the **Latest News** link changed to **Latest Alerts**. The associated bell-shaped icon now displays a red dot to indicate new messages. Click **Latest Alerts** to read the news or alerts about Symantec Endpoint Protection. The link goes to: **Endpoint Protection Notifications**

**System requirements**

Symantec Endpoint Protection 14.0.1 MP1 adds support for:

- Third-party component upgrades, including Java SE Development Kit 8, zlib, and Commons-Jelly.
- Symantec Endpoint Protection Manager web console: Mozilla Firefox 5.x through 57.x, Google Chrome 63.0.x

See “**System requirements for Symantec Endpoint Protection**” on page 15.

**REST API commands**

The documentation for the Symantec Endpoint Protection Manager REST APIs is now available in the following locations:

  - You can access this location from the cloud portal Help by clicking the last icon at the bottom of the dashboard.

**Note:** If Symantec Endpoint Protection Manager is enrolled with the cloud portal, using REST API commands to manage what the cloud portal manages is not supported.

- On the Symantec Endpoint Protection Manager server at the following address, where `SEPM-IP` is the IP address of the Symantec Endpoint Protection Manager server:

**Product guides for all versions of Symantec Endpoint Protection 14**

**Removed or unsupported features**

- **End-of-Support for Network Access Control**
  - Symantec discontinued technical support and content updates for customers with current Basic Maintenance Support or Essential Support on November 5, 2017 for Symantec Network Access Control, Symantec Network Access Control Starter Edition, and Symantec
Network Access Control Enforcer with 6100 Series Appliance. Host Integrity has already been integrated in Symantec Endpoint Protection.

Symantec Network Access Control (SNAC) End of Life FAQ for Customers and Partners
Announcing the End of Life of Symantec Network Access Control 12.1

Known issues and workarounds

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

- See “Upgrade information” on page 9.
- See “Client information” on page 10.
- See “Symantec Endpoint Protection Manager information” on page 10.
- See “Documentation and help information” on page 15.

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

New fixes and component versions in Symantec Endpoint Protection 14.0.1 MP1

Upgrade information

This section contains information about upgrading to the current release of the product.

The upgrade to 14.0.x from 12.1.x prompts for database credentials

When you upgrade a from a 12.1.x to 14.0.x Symantec Endpoint Protection Manager that uses a SQL Server database, the wizard now prompts you for system administrator credentials. You should enter the appropriate credentials for access to the SQL Server, and then continue with the upgrade.

The upgrade from 14 to a later version does not prompt for these credentials.

Security patches are not included when you restore a 12.1.x database to 14.0.x

If you upgrade to Symantec Endpoint Protection Manager 14.0.x and you use a database that you restore from version 12.1.x, you do not get the following:

- Version 14.0.x client installation packages
- Security patches
  See Downloading Endpoint Protection security patches to Windows clients for information.

To get the 14.0.x client installation packages, you must manually import them on the Admin pane > Install Packages tab.

Importing client installation packages into Symantec Endpoint Protection Manager
To get the version 14.0.x security patches, however, you must copy the patches from the installation file that you download from FileConnect.

To copy security patches to a version 14.0.x management server

1. After you download and extract the Symantec Endpoint Protection full installation file from FileConnect, copy the contents of the \SEPM\Packages folder to the SEPM-install\tomcat\packages folder.

   SEPM-install represents the Symantec Endpoint Protection Manager installation path.

   For information on how to download from FileConnect, see: Download the latest version of Symantec Endpoint Protection.

2. In the SEPM-install\bin folder, run upgrade.bat.

An unmanaged client appears in the cloud portal after an upgrade with a package with Hardening policies

You upgrade an unmanaged Symantec Endpoint Protection client with a default managed client package. You exported this package from a cloud portal-enrolled Symantec Endpoint Protection Manager with custom policies that include a Hardening policy. By default, this client computer should remain unmanaged. However, this unmanaged client appears in the default group in the cloud portal.

To avoid this situation, upgrade an unmanaged Symantec Endpoint Protection client with a default unmanaged client package.

Installing an unmanaged Windows client

Client information

This section contains information about the Symantec Endpoint Protection client for Windows, Mac, or Linux.

Earlier Symantec Endpoint Protection Manager 14 versions cannot manage Symantec Endpoint Protection 14.0.1 or later Windows clients

You must manage Symantec Endpoint Protection 14.0.1 (14 RU1) or later Windows clients with a Symantec Endpoint Protection Manager that also runs version 14.0.1 or later. Symantec Endpoint Protection Manager for versions 14, 14 MP1, and MP2 cannot correctly manage the versions later than 14.0.1, including 14.0.1 MP1.

No workaround exists for this scenario.

Symantec Endpoint Protection Manager information

This section contains information about Symantec Endpoint Protection Manager.
Remote Java Console access to Symantec Endpoint Protection Manager fails with FIPS enabled

In a FIPS-compliant environment, access to Symantec Endpoint Protection Manager 14.0.1 MP1 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

Use of the cloud portal in a FIPS-enabled environment is not supported

Enrollment with and use of the cloud portal is not supported when you configure Symantec Endpoint Protection Manager 14.0.1 MP1 for FIPS 140-2 compliance.

Symantec Endpoint Protection 14 FIPS 140-2 Deployment Guide

Cannot access Symantec Endpoint Protection Manager Web Console with the Edge browser on Windows 10 (32-bit)

The Edge browser on the 32-bit version of Windows 10 does not support plug-ins. Therefore, you cannot launch the Symantec Endpoint Protection Manager Web Console, which requires Java. To access the Symantec Endpoint Protection Manager by web console, use another supported browser, such as Internet Explorer 11 or Firefox.

See “Symantec Endpoint Protection Manager system requirements” on page 16.

How Symantec Endpoint Protection Manager interacts with the cloud portal

This section lists some expected behaviors that may occur when you enroll a Symantec Endpoint Protection Manager domain in the cloud portal.

Connections and enrollment between the cloud portal and Symantec Endpoint Protection Manager

- If the Symantec Endpoint Protection Manager connector cannot obtain the access token to the cloud portal, it retries every hour.
- Clients that connect through Symantec Endpoint Protection Manager may not immediately display the correct online status in the cloud portal. Allow for 5-10 minutes after the online status changes to see an accurate reflection of the current status.
- The system time for the management server and the AWS must be within 10 minutes of each other. Otherwise, enrollment fails, and you see the following error message:
Enrollment in Security Cloud cannot complete because the Symantec Endpoint Protection Manager computer date and time does not match the current date and time. Change the setting in the Control Panel, and then retry the enrollment.

To resolve the time mismatch, synchronize the Symantec Endpoint Protection Manager server with Network Time Protocol (NTP). See the following for more information:
http://www.ntp.org

You can use the following logs to troubleshoot a failed enrollment: BRIDGE_INSTALL.log, catalinaWs.out, Cloud-0.log, scm-server-0.log, and semapisrv_access_log.date.log. All of these files are in \tomcat\logs, within the Symantec Endpoint Protection Manager installation folder.

License, installation, upgrading, database

- You do not need a separate license to use or enroll in the cloud portal; the cloud portal license is free. You only need a license for Symantec Endpoint Protection.
- You cannot upgrade a management server from the cloud portal.
- You cannot back up or restore the embedded database or Symantec Endpoint Protection Manager settings from the cloud. You still back up and restore the database and settings in Symantec Endpoint Protection Manager.
- To free up licenses, the Symantec Endpoint Protection Manager database deletes the clients that have not connected to the domain, based on the number of days that you specify. In the cloud portal, these clients are automatically deleted after 30 days, and you cannot configure this interval. The clients are deleted first in the Symantec Endpoint Protection Manager database and then in the cloud portal.

Domains, sites, replication

- For each site, you enroll one Symantec Endpoint Protection Manager domain per site in the cloud portal. You cannot enroll multiple domains even if the domains are in separate sites. You also cannot enroll separate Symantec Endpoint Protection Manager domains if you use the same cloud portal account.
- For sites with two Symantec Endpoint Protection Managers that share a SQL Server database and that are configured for failover, you enroll one domain from each management server. The bridge service that communicates between each management server and the cloud portal runs on one management server at a time. The service runs on the management server with the higher server priority first. If the first bridge service goes down, the service to the second management server runs instead. You can only manage one domain at a time from the cloud portal. The sync between the cloud portal and each management server does occur simultaneously.

Table 1-1 displays which site configurations the cloud portal supports when you enroll a Symantec Endpoint Protection Manager domain.
Table 1-1 Site configurations that the cloud portal supports

<table>
<thead>
<tr>
<th>Site configuration</th>
<th>Supported on the cloud portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>One site, one Symantec Endpoint Protection Manager on one computer with an embedded database only</td>
<td>Yes</td>
</tr>
<tr>
<td>One site, one Symantec Endpoint Protection Manager on one computer with a Microsoft SQL Server database on the second computer</td>
<td>Yes</td>
</tr>
<tr>
<td>One site, multiple Symantec Endpoint Protection Managers</td>
<td>Yes</td>
</tr>
<tr>
<td>Multiple sites, one Symantec Endpoint Protection Manager, with replication</td>
<td>No</td>
</tr>
<tr>
<td>Multiple sites, multiple Symantec Endpoint Protection Managers, with replication</td>
<td>No</td>
</tr>
</tbody>
</table>

**Groups, clients, locations**

- If you rename **My Company** in the cloud portal, the group name does not change in Symantec Endpoint Protection Manager.

- Cloud-managed features require a managed client. You cannot manage an unmanaged client or apply a policy that uses cloud features to an unmanaged client. If you apply policies that use cloud features to an unmanaged client, the policy defaults to the equivalent legacy Symantec Endpoint Protection options.

- Version 14, 14 MP1, 14 MP2 and legacy 12.1.x client computers appear in the cloud portal, but do not support any of the new cloud-based features.

- If the Manage Devices switch is on in the cloud portal, the cloud portal manages the devices. If it is off, then Symantec Endpoint Protection Manager manages the devices. If you use Active Directory with Symantec Endpoint Protection Manager to manage groups and clients, then Symantec Endpoint Protection Manager automatically manages devices. In this case, you cannot switch Manage Devices to the cloud portal.

- Whenever you make a change to the device group structure, there is a 10-minute delay before the change appears in Symantec Endpoint Protection Manager. The reverse is also true. The behavior is similar to how Symantec Endpoint Protection Manager replication functions. During the delay, you should not try to make additional topology changes.

- If you add a group or policy in the cloud portal that contains any of the following special characters: `/ \ * ? < > | : "`, these characters are converted to a dash in the Symantec Endpoint Protection Manager. For example, if you name a group **Europe***, on Symantec Endpoint Protection Manager, this group is labeled as **Europe---**.

- The cloud portal does not support locations. Therefore, if a Symantec Endpoint Protection Manager group has multiple locations and each location uses a different policy (shared or non-shared), then only the default location’s policy gets synched up and applied to the
equivalent group on the cloud portal. After the cloud portal syncs back with Symantec
Endpoint Protection Manager, that group’s policy in the cloud portal is applied as a shared
policy to all the locations in the equivalent group on the Symantec Endpoint Protection
Manager. This process applies to both the Memory Exploit Mitigation policy and the
Exceptions policy in the Symantec Endpoint Protection Manager.

Policies and inheritance

- You can only manage policy settings for 14.0.1/14.1 and 14.0.1 MP1 clients from the cloud.
  You must still manage policy settings for clients earlier than 14.0.1 directly from Symantec
  Endpoint Protection Manager. However, there are exceptions. If you apply an Exceptions
  policy from the cloud, and the client supports the exception type, then the exception applies
to the client regardless of version. Memory Exploit Mitigation policies apply to all version
14 clients and later.

- Policies that come from the cloud do not follow the policy inheritance configuration for
  Symantec Endpoint Protection Manager. Instead, they follow the inheritance rules that are
  defined in the cloud.

- In the Virus and Spyware Protection policy, a cloud icon appears next to some options
  when the domain is enrolled in the cloud portal. If an Intensive Protection policy is in effect,
  the policy overrides these options for 14.0.1/14.1 and 14.0.1 MP1 clients only.

- If you assign a cloud-based policy to a group with no clients, Symantec Endpoint Protection
  Manager does not display the policy or any policy changes to that group. The group must
  have at least one client to receive the cloud-based policy changes.

- The first default cloud policies that you create and assign in the cloud portal is appended
  with a v and a number (#) in Symantec Endpoint Protection Manager, as follows: Default
  MEM Policy v1. If you then unenroll and then reenroll the Symantec Endpoint Protection
  Manager domain, an additional v# is appended to the policy name. For example, Default
  MEM Policy v1 may become Default MEM Policy v1 v1 or Default MEM Policy v1 v3.

- For differences between the Symantec Endpoint Protection Manager Exceptions policy
  and the cloud portal Blacklist and Whitelist policies:

Clients do not automatically upgrade when updating client patches

In version 14, a new feature was added to Symantec Endpoint Protection Manager so that
LiveUpdate could download the critical security updates that Symantec determined should not
wait until a new version of the Windows client was available. However, an unintended
consequence was that if you upgraded to a new build of the same version of Symantec Endpoint
Protection Manager, such as from 14 MP1 to 14 MP1a, the clients with same version as
Symantec Endpoint Protection Manager would unexpectedly and automatically upgrade. In
14.0.1, Symantec fixed this issue so that the clients do not automatically upgrade.
Downloading Endpoint Protection security patches to Windows clients

Localization support for Symantec Endpoint Protection Hardening
Symantec Endpoint Protection Hardening policies are not supported for use for localized versions of Symantec Endpoint Protection 14.0.1 or for localized operating systems. Support is planned for a future Symantec Endpoint Protection release.

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

Finding non-English documentation
To find documentation in non-English languages, the Release_Notes.html file that is installed with Symantec Endpoint Protection Manager points you to the main Symantec Documentation Page. Instead, click the links in this topic:

See “Where to get more information” on page 27.

Symantec does not have separate documentation pages for Czech, Polish, and Russian. You can find the documentation for these languages on the English page.

To find the documentation for Czech, Polish, or Russian
1. Go to the English page: Symantec Product Documentation, click the All Versions drop-down list, and choose the release number for the documentation you want.
2. Under each guide, click Download, click the link for the language you want, and then click Open.
   Not all guides are translated into all languages.

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 14.0.1
- See “Symantec Endpoint Protection Manager system requirements” on page 16.
- See “Symantec Endpoint Protection client for Windows system requirements” on page 19.
- See “Symantec Endpoint Protection client for Windows Embedded system requirements” on page 22.
- See “Symantec Endpoint Protection client for Mac system requirements” on page 23.
- See “Symantec Endpoint Protection client for Linux system requirements” on page 23.

See “Supported virtual installations and virtualization products” on page 25.

Symantec Endpoint Protection Manager system requirements

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

### Table 1-2 Symantec Endpoint Protection Manager software system requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Operating system  | - Windows Server 2008 (64-bit)  
|                   |   - Windows Server 2008 R2                                                   |
|                   |   - Windows Server 2012                                                     |
|                   |   - Windows Server 2012 R2                                                   |
|                   |   - Windows Server 2016                                                     |
|                   | **Note:** Desktop operating systems are not supported. Window Server Core edition is not supported. Windows Server Core does not include Internet Explorer, which Symantec Endpoint Protection Manager requires to work. |
| Web browser       | The following browsers are supported for web console access to Symantec Endpoint Protection Manager and for viewing the Symantec Endpoint Protection Manager Help: |
|                   |   - Microsoft Edge  
|                   |     **Note:** The 32-bit version Windows 10 does not support web console access on the Edge browser. |
|                   |     See "Cannot access Symantec Endpoint Protection Manager Web Console with the Edge browser on Windows 10 (32-bit)" on page 11. |
|                   |   - Microsoft Internet Explorer 11                                    |
|                   |   - Mozilla Firefox 5.x through 57.x                                    |
|                   |   - Google Chrome 63.x                                                  |
### Table 1-2  
**Symantec Endpoint Protection Manager software system requirements (continued)**

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Database  | The Symantec Endpoint Protection Manager includes an embedded database. You may instead choose to use a database from one of the following versions of Microsoft SQL Server:  
- SQL Server 2008, SP4  
- SQL Server 2008 R2, SP3  
- SQL Server 2012, RTM - SP4  
- SQL Server 2014, RTM - SP2  
- SQL Server 2016, RTM, SP1  
- SQL Server 2017  

**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](#) |

### Table 1-3  
**Symantec Endpoint Protection Manager hardware system requirements**

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| 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 |
**Table 1-3**  Symantec Endpoint Protection Manager hardware system requirements (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Hard drive when installing to the system drive | With an embedded database or a local SQL Server database:  
  - 40 GB available minimum (200 GB recommended) for the management server and database  
  With a remote SQL Server database:  
  - 40 GB available minimum (100 GB recommended) for the management server  
  - Additional available disk space on the remote server for the database |
| Hard drive when installing to an alternate drive | With an embedded database or a local SQL Server database:  
  - The system drive requires 15 GB available minimum (100 GB recommended)  
  - The installation drive requires 25 GB available minimum (100 GB recommended)  
  With a remote SQL Server database:  
  - The system drive requires 15 GB available minimum (100 GB recommended)  
  - The installation drive requires 25 GB available minimum (100 GB recommended)  
  - Additional available disk space on the remote server for the database |

**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 25.
## Symantec Endpoint Protection client for Windows system requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system (desktop)</td>
<td>■ Windows Vista (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 7 (32-bit, 64-bit; RTM and SP1)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 8 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Embedded 8 Standard (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 8.1 (32-bit, 64-bit), including Windows To Go</td>
</tr>
<tr>
<td></td>
<td>■ Windows 8.1 update for April 2014 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 8.1 update for August 2014 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 10 (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 10 Anniversary Update (2016) (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 10 Creators Update (2017) (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows 10 Fall Creators Update (2017) (32-bit, 64-bit)</td>
</tr>
<tr>
<td></td>
<td>See “Symantec Endpoint Protection client for Windows Embedded system requirements” on page 22.</td>
</tr>
<tr>
<td>Operating system (server)</td>
<td>■ Windows Server 2008 (32-bit, 64-bit; R2, SP1, and SP2)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Small Business Server 2008 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Essential Business Server 2008 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Small Business Server 2011 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012 R2 update for April 2014</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2012 R2 update for August 2014</td>
</tr>
<tr>
<td></td>
<td>■ Windows Server 2016</td>
</tr>
<tr>
<td>Browser Intrusion Prevention</td>
<td>Browser Intrusion Prevention support is based on the version of the Client Intrusion Detection System (CIDS) engine.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Supported browsers for Browser Intrusion Prevention in Endpoint Protection.</td>
</tr>
</tbody>
</table>
### Table 1-5  
Symantec Endpoint Protection client for Windows hardware system requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>■ 32-bit processor: 2 GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended)</td>
</tr>
</tbody>
</table>
|               | ■ 64-bit processor: 2 GHz Pentium 4 with x86-64 support or equivalent minimum  
  
  **Note:** Itanium processors are not supported. |
| 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.  
  
  **Hard drive system requirements:**  
  
  ■  Table 1-6 describes the hard drive system requirements when Symantec Endpoint Protection is installed to the system drive.  
  
  ■  Table 1-7 describes the hard drive system requirements when Symantec Endpoint Protection is installed to an alternate drive.  
  
  **Note:** Space requirements are based on NTFS file systems. Additional space is also required for content updates and logs. |

### Table 1-6  
Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to the system drive

<table>
<thead>
<tr>
<th>Client type</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| 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 |
Table 1-6  Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to the system drive (continued)

<table>
<thead>
<tr>
<th>Client type</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded / VDI</td>
<td>With the program data folder located on the system drive:</td>
</tr>
<tr>
<td></td>
<td>■ 245 MB*</td>
</tr>
<tr>
<td></td>
<td>With the program data folder located on an alternate drive:</td>
</tr>
<tr>
<td></td>
<td>■ System drive: 180 MB</td>
</tr>
<tr>
<td></td>
<td>■ Alternate installation drive: 200 MB</td>
</tr>
<tr>
<td>Dark network</td>
<td>With the program data folder located on the system drive:</td>
</tr>
<tr>
<td></td>
<td>■ 545 MB*</td>
</tr>
<tr>
<td></td>
<td>With the program data folder located on an alternate drive:</td>
</tr>
<tr>
<td></td>
<td>■ System drive: 180 MB</td>
</tr>
<tr>
<td></td>
<td>■ Alternate installation drive: 500 MB</td>
</tr>
</tbody>
</table>

* An additional 135 MB is required during installation.

Table 1-7  Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to an alternate drive

<table>
<thead>
<tr>
<th>Client type</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>With the program data folder located on the system drive:</td>
</tr>
<tr>
<td></td>
<td>■ System drive: 380 MB</td>
</tr>
<tr>
<td></td>
<td>■ Alternate installation drive: 15 MB*</td>
</tr>
<tr>
<td></td>
<td>With the program data folder located on an alternate drive:**</td>
</tr>
<tr>
<td></td>
<td>■ System drive: 30 MB</td>
</tr>
<tr>
<td></td>
<td>■ Program data drive: 350 MB</td>
</tr>
<tr>
<td></td>
<td>■ Alternate installation drive: 150 MB</td>
</tr>
<tr>
<td>Embedded / VDI</td>
<td>With the program data folder located on the system drive:</td>
</tr>
<tr>
<td></td>
<td>■ System drive: 230 MB</td>
</tr>
<tr>
<td></td>
<td>■ Alternate installation drive: 15 MB*</td>
</tr>
<tr>
<td></td>
<td>With the program data folder located on an alternate drive:**</td>
</tr>
<tr>
<td></td>
<td>■ System drive: 30 MB</td>
</tr>
<tr>
<td></td>
<td>■ Program data drive: 200 MB</td>
</tr>
<tr>
<td></td>
<td>■ Alternate installation drive: 150 MB</td>
</tr>
</tbody>
</table>
Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to an alternate drive (continued)

<table>
<thead>
<tr>
<th>Client type</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dark network</td>
<td>With the program data folder located on the system drive:</td>
</tr>
<tr>
<td></td>
<td>■ System drive: 530 MB</td>
</tr>
<tr>
<td></td>
<td>■ Alternate installation drive: 15 MB*</td>
</tr>
<tr>
<td></td>
<td>With the program data folder located on an alternate drive:**</td>
</tr>
<tr>
<td></td>
<td>■ System drive: 30 MB</td>
</tr>
<tr>
<td></td>
<td>■ Program data drive: 500 MB</td>
</tr>
<tr>
<td></td>
<td>■ Alternate installation drive: 150 MB</td>
</tr>
</tbody>
</table>

* 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.

See “Supported virtual installations and virtualization products” on page 25.

Symantec Endpoint Protection client for Windows Embedded system requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>1 GHz Intel Pentium</td>
</tr>
<tr>
<td>Physical RAM</td>
<td>256 MB</td>
</tr>
<tr>
<td>Embedded operating system</td>
<td>■ Windows Embedded Standard 7 (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Embedded POSReady 7 (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Embedded Enterprise 7 (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Embedded 8 Standard (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Embedded 8.1 Industry Pro (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Embedded 8.1 Industry Enterprise (32-bit and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Embedded 8.1 Pro (32-bit and 64-bit)</td>
</tr>
<tr>
<td>Required minimum components</td>
<td>■ Filter Manager (FltMgr.sys)</td>
</tr>
<tr>
<td></td>
<td>■ Performance Data Helper (pdh.dll)</td>
</tr>
<tr>
<td></td>
<td>■ Windows Installer Service</td>
</tr>
</tbody>
</table>
**Table 1-8**  Symantec Endpoint Protection client for Windows Embedded system requirements (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| 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 “Supported virtual installations and virtualization products” on page 25.

**Symantec Endpoint Protection client for Mac system requirements**

**Table 1-9**  Symantec Endpoint Protection client for Mac system requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>64-Bit Intel Core 2 Duo or later</td>
</tr>
<tr>
<td>Physical RAM</td>
<td>2 GB of RAM</td>
</tr>
<tr>
<td>Hard drive</td>
<td>500 MB of available hard disk space for the installation</td>
</tr>
<tr>
<td>Display</td>
<td>800 x 600</td>
</tr>
<tr>
<td>Operating system</td>
<td>Mac OS X 10.10, 10.11; macOS 10.12, 10.13</td>
</tr>
</tbody>
</table>

**Symantec Endpoint Protection client for Linux system requirements**

**Table 1-10**  Symantec Endpoint Protection client for Linux system requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Hardware  | ■ Intel Pentium 4 (2 GHz) or later processor  
                     ■ 1 GB of RAM  
                     ■ 7 GB of available hard disk space |
### System requirements for Symantec Endpoint Protection

#### Operating systems
- Amazon Linux
- CentOS 6U3 - 6U9, 7 - 7U4; 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, 7, 7U1, 7U2, 7U3
- Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U4
- 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; 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

#### Other environmental requirements
- Glibc
  - Any operating system that runs glibc earlier than 2.6 is not supported.
- i686-based dependent packages on 64-bit computers
  - Many of the executable files in the Linux client are 32-bit programs. For 64-bit computers, you must install the i686-based dependent packages before you install the Linux client.
  - If you have not already installed the i686-based dependent packages, you can install them by command line. This installation requires superuser privileges, which the following commands demonstrate with `sudo`:
    - **For Red Hat-based distributions:**
      ```
      sudo yum install glibc.i686 libgcc.i686 libX11.i686
      ```
    - **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 or iproute2
  - Symantec Endpoint Protection uses one of these two tools, depending on what is already installed on the computer.
- XFS file systems that contain inode64 attributes are not supported.

See “Supported virtual installations and virtualization products” on page 25.
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
- VMware ESXi 6.0 Update 3
- VMware ESXi 6.5
- Microsoft Virtual Server 2005
- 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 14.0.1 MP1:
- 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 MP9 (12.1.7369.6900)
- 14 (14.0.1904.0000)
- 14 MP1 (14.0.2332.0100) or 14 MP1 Refresh Build (14.0.2349.0100)
- 14 MP2 (14.0.2415.0200)
- 14.0.1 (14.0.3752.1000)

**Mac client**
The following versions of Symantec Endpoint Protection client for Mac can upgrade directly to 14.0.1 MP1:
- 12.1.4 - 12.1.6 MP9 (12.1.7369.6900)
- 14 (14.0.1904.0000)
- 14 MP1 (14.0.2349.0100 or 14.0.2332.0100)
- 14 MP2 (14.0.2415.0200)
- 14.0.1 (14.0.3752.1000)

**Linux client**
The following versions of Symantec Endpoint Protection client for Linux can upgrade directly to 14.0.1 MP1:
- 12.1.x, up to 12.1.6 MP9 (12.1.7369.6900)
- 14 (14.0.1904.0000)
- 14 MP1 (14.0.2349.0100 or 14.0.2332.0100)
- 14 MP2 (14.0.2415.0200)
- 14.0.1 (14.0.3752.1000)

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

Versions of Symantec Endpoint Protection for Mac earlier than 12.1.4

You cannot upgrade Symantec Endpoint Protection Manager 11.0.x or Symantec Endpoint Protection Manager Small Business Edition 12.0.x directly 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 14.0.x.

Downgrade paths are not supported. For example, if you want to migrate from Symantec Endpoint Protection 14 MP2 to 12.1.6 MP9, you must first uninstall Symantec Endpoint Protection 14 MP2.

**Where to get more information**

Table 1-11 displays the websites where you can get best practices, troubleshooting information, and other resources to help you use the product.

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Website link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trial versions</td>
<td>Trialware (14.x)</td>
</tr>
<tr>
<td>Manuals and documentation updates</td>
<td><strong>English:</strong></td>
</tr>
<tr>
<td></td>
<td>▪ Symantec Product Documentation</td>
</tr>
<tr>
<td></td>
<td>▪ Product guides for all versions of Symantec Endpoint Protection 14</td>
</tr>
<tr>
<td></td>
<td><strong>Other languages:</strong></td>
</tr>
<tr>
<td></td>
<td>▪ Brazilian Portuguese</td>
</tr>
<tr>
<td></td>
<td>▪ Chinese (simplified)</td>
</tr>
<tr>
<td></td>
<td>▪ Chinese (traditional)</td>
</tr>
<tr>
<td></td>
<td>▪ French</td>
</tr>
<tr>
<td></td>
<td>▪ German</td>
</tr>
<tr>
<td></td>
<td>▪ Italian</td>
</tr>
<tr>
<td></td>
<td>▪ Japanese</td>
</tr>
<tr>
<td></td>
<td>▪ Korean</td>
</tr>
<tr>
<td></td>
<td>▪ Spanish</td>
</tr>
<tr>
<td></td>
<td>*Czech, Polish, and Russian files are on the English page.</td>
</tr>
<tr>
<td>Technical Support</td>
<td>Endpoint Protection Technical Support</td>
</tr>
<tr>
<td></td>
<td>Includes knowledge base articles, product release details, updates and patches, and contact options for support.</td>
</tr>
<tr>
<td>Threat information and updates</td>
<td>Symantec Security Center</td>
</tr>
<tr>
<td>Types of information</td>
<td>Website link</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Training</td>
<td>- Symantec Education Services</td>
</tr>
<tr>
<td></td>
<td>Access the training courses, the eLibrary, and more.</td>
</tr>
<tr>
<td>Symantec Connect forums</td>
<td>Endpoint Protection</td>
</tr>
</tbody>
</table>