Symantec™ Endpoint Protection, Symantec Endpoint Protection Small Business Edition, and Symantec Network Access Control 12.1.4 Release Notes

Symantec Endpoint Protection, Symantec Endpoint Protection Small Business Edition, and Symantec Network Access Control Release Notes

Product version: 12.1.4

Documentation version: 1

This document was last updated on: October 30, 2013 at 11:31

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_apac@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 the following product editions:

- Symantec Endpoint Protection, enterprise version
- Symantec Endpoint Protection Small Business Edition
- Symantec Network Access Control

You should assume that all the material applies to all editions, unless otherwise noted.

Review this document before you install these products, or before you call Technical Support. The release notes describe known issues and provide the additional information that is not included in the standard documentation or the context-sensitive Help.

You can find the latest version of the release notes and system requirements at the following URL:

Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

What's new in Symantec Endpoint Protection 12.1.4 (12.1 RU4)

Note: Symantec Endpoint Protection 12.1.4 is the last release update to support Symantec Protection Center 1.0. Support continues in future release updates for Symantec Protection Center 2.0 and the Symantec Endpoint Protection Manager web console.

Table 1-1 describes the new features for this release.

Table 1-1 New features in Symantec Endpoint Protection 12.1.4

Feature	Benefit
Expanded operating system and browser support	■ Supports Mac OS X 10.9 and Windows 8.1 / Server 2012 R2. ■ Supports the latest versions of Internet Explorer, Firefox, and Chrome.
Enhanced support for remote deployment for Mac	Supports the creation of installation packages for use with Mac-based third-party remote client management and distribution systems. This added support includes: ■ A standardized, independent package that requires no additional files or scripts for remote deployment ■ Remote deployment to target Mac computers on which no user is logged on ■ Support for unattended installation ■ Support for silent installation
Intrusion prevention for Mac	You can deploy intrusion prevention protection to Mac client computers. Intrusion prevention analyzes the network traffic with the use of the intrusion prevention signatures to block attacks or patterns of attack.
LiveUpdate 6 for Mac	The Mac client includes LiveUpdate 6, which no longer depends on Java to run. LiveUpdate-related tasks run even if no user is logged in. LiveUpdate-related tasks include a scheduled LiveUpdate launch.

Table 1-1 New features in Symantec Endpoint Protection 12.1.4 *(continued)*

Feature	Benefit
Improved scheduled scan options for Mac	Scheduled scan options for Mac match the options available for Windows clients. The end user can pause, snooze, and cancel a scheduled scan from the Mac client user interface.
Content for Mac from Symantec Endpoint Protection Manager	You can configure the Symantec Endpoint Protection Manager Apache web server to allow Mac clients to download LiveUpdate content. For configuration instructions, see the following webpage: Enabling Mac clients to download LiveUpdate content using the Apache Web server as a reverse proxy
User interface improvements for Mac	The Mac client user interface is more consistent both with Apple style and with the Symantec conventions.
Additional language support for Mac	In addition to English, French, Italian, German, Spanish, and Japanese, the Mac client supports the following languages: ■ Chinese (traditional) ■ Chinese (simplified) ■ Korean ■ Brazilian Portuguese
Symantec Endpoint Protection Manager 12.1.2 management support for the 12.1.4 Mac client	If you are not able to immediately upgrade your management server, you can manage the Symantec Endpoint Protection 12.1.4 Mac client with Symantec Endpoint Protection Manager 12.1.2. However, Symantec Endpoint Protection Manager 12.1.2 can only support the Symantec Endpoint Protection 12.1.4 Mac client at the level of protection technology available for version 12.1.2.
Faster alerting and notifications for priority events	Symantec Endpoint Protection Windows clients can quickly send priority events to Symantec Endpoint Protection Manager without waiting for the next heartbeat. You can also create notifications without a damper for critical events. Priority events include malware infections and IPS alerts.
Support for Lotus Notes 9.0 (enterprise version)	Auto-Protect Email Protection for Lotus Notes supports Lotus Notes 9.0.
Support for ESXi 5.1 Update 1 (enterprise version)	Supports the use of ESXi 5.1 Update 1 with vShield Endpoint 5.1.

Known issues and workarounds

The issues in this section apply to the most current version of the product.

- Known issues about upgrades, migration, and installation.
  See "Installation, upgrade, and migration issues" on page 9.
- Known issues about the Symantec Endpoint Protection client.
  See "Client issues" on page 10.
- Known issues about Symantec Network Access Control only. This section includes those issues about the Enforcer and Host Integrity policies.
  See "Symantec Network Access Control, Enforcers, and Host Integrity issues" on page 11.
- Documentation changes and updates for any one of the versions.
  See "Documentation changes and updates" on page 11.

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

New fixes and features in Symantec Endpoint Protection 12.1 Release Update 4 (12.1 RU4)

Installation, upgrade, and migration issues

This section contains information about installation, upgrades, and migration.

Installing on and upgrading to Windows 8.1 / Windows Server 2012 R2 with Symantec Endpoint Protection

Symantec Endpoint Protection 12.1.4 is the only Symantec Endpoint Protection version that supports Windows 8.1 / Windows Server 2012 R2.

Symantec Endpoint Protection 12.1.4 supports the upgrade from Windows 8 to Windows 8.1 with the Symantec Endpoint Protection 12.1.4 client installed.

Symantec Endpoint Protection 12.1.4 does not support the following upgrade paths:

- Windows versions earlier than 8 to Windows 8 with the Symantec Endpoint Protection 12.1.4 client installed; for example, Windows 7 to Windows 8
- Windows 8 to Windows 8.1 with Symantec Endpoint Protection Manager 12.1.4 installed
- Windows Server 2012 to Windows Server 2012 R2 with the Symantec Endpoint Protection 12.1.4 client or Symantec Endpoint Protection Manager 12.1.4 installed

In these scenarios, you must uninstall the Symantec Endpoint Protection 12.1.4 before you upgrade the operating system.

The Symantec Uninstaller backs up the quarantine.qtn file to an unexpected folder on Symantec Endpoint Protection Mac clients (3145213)

Typically, the Symantec Uninstaller backs up the quarantine in a `quarantine.qtn` file located in the `/Users/`*`username`*`/Desktop/Saved Symantec Data` folder. Because of some limitations in the Uninstaller, however, the `quarantine.qtn` file is now backed up to the `/Users/Shared/Saved Symantec Data` folder.

When you reinstall, the Mac client automatically restores the backup of the quarantine file to the correct location.

Client issues

This section contains information about the Symantec Endpoint Protection client on the Windows platform.

After Symantec Endpoint Protection client installation, a message about Windows Defender appears in logs every five minutes (3331236)

After you install the Symantec Endpoint Protection client on Windows 8.1, you see that the following message is written to the Application event log every five minutes: "The Windows Security Center Service could not stop Windows Defender." This message is informational only, and you can safely disregard it.

Microsoft resolved this issue in the following build: 9650.0.fbl_sid_auth.131021-1730.

When you migrate from Windows 8 to Windows 8.1, the client service (`smc`) gets removed (3344637)

If the Symantec Endpoint Protection client is installed on a drive other than C:\, and you migrate the client operating system from Windows 8 to Windows 8.1, the client service gets removed.

To work around this issue, perform the following steps after you migrate the client computer from Windows 8 to Windows 8.1.

To reinstall the client service

1. Repair the client service by clicking **Add/Remove Programs**, right-clicking **Symantec Endpoint Protection**, and clicking **Repair**.
2. Reinstall the Teefer driver.

   See Installing Teefer manually.
3. Restart the client computer.

Symantec is working on this issue with Microsoft.

Symantec Network Access Control, Enforcers, and Host Integrity issues

This section contains information about Symantec Network Access Control, Enforcers, and Host Integrity.

Download of the Symantec Network Access Control On-Demand client fails with Internet Explorer 11 on Windows 8.1 / Windows Server 2012 R2 (3212661)

When you use Internet Explorer 11 to download and install the Symantec Network Access Control On-Demand client on Windows 8.1 / Windows Server 2012 R2 from the Gateway Enforcer, the download fails.

To work around the issue, right-click Internet Explorer 11, click **Run as administrator**, and then download the Symantec Network Access Control On-Demand client. You can also uncheck **Enable Protected Mode** under **Tools > Internet Options > Security**, and then restart Internet Explorer 11 to download.

802.1x authentication fails after you install the Symantec Network Access Control On-Demand client on Windows 8.1 / Windows Server 2012 R2 (3164704)

When you use Firefox to download and install the Symantec Network Access Control On-Demand client on Windows 8.1 / Windows Server 2012 R2 from the Gateway Enforcer, 802.1x authentication does not function.

To work around the issue, right-click Firefox, click **Run as administrator**, and then download the Symantec Network Access Control On-Demand client.

Documentation changes and updates

This section describes documentation changes that apply to the PDFs and the online Help. Unless otherwise specified, the original content appears in the *Symantec Endpoint Protection and Symantec Network Access Control Installation and Administration Guide*, the *Symantec Endpoint Protection Small Business Edition Installation and Administration Guide*, and the Symantec Endpoint Protection Manager Help.

Symantec updates the Support page with the changed content, but not in the PDFs or online Help until the next major release.

Table 1-2 Documentation and Help updates

Topic heading	Text change
A change in a client group no longer triggers a notification (2915552)	The section "What are the types of notifications and when are they sent?" contains incorrect information. A change in a client group no longer triggers a notification.
The Windows client help incorrectly identifies columns for definition version troubleshooting (2951158)	In the client, if you click **Help > Troubleshooting > Versions > Help**, the documentation incorrectly includes the version number and moniker in the **Definitions** columns description. The columns display information for the type, sequence number, and the last-checked date of the currently installed virus definition files and other definitions files.
"What's New in Symantec Network Access Control 12.1.2" lists support for an unsupported switch	In the *Symantec Network Access Control 12.1.2 Getting Started Guide*, the section "What's New in Symantec Network Access Control 12.1.2" incorrectly lists the Dell Force 10 as a supported switch.
Documentation for Network Access Control third-party enforcement solutions incorrectly lists Cisco NAC (Network Access Control) (2640641)	The section "How does enforcement manage computers without clients?" incorrectly lists the Cisco NAC as a supported third-party enforcement solution for Symantec Network Access Control.
System administrator credentials must be used when you re-add an existing replication partner (enterprise version) (3073261)	The section "Re-adding a replication partner that you previously deleted" does not specify that you must use system administrator credentials. You cannot use domain administrator or limited administrator credentials.
Help for Application Control scan exclusion does not list the ability to exclude child processes (enterprise version) (3076607)	You can now exclude child processes when you exclude a Windows file from an Application Control scan in an Exceptions policy. This capability is a new enhancement as of Symantec Endpoint Protection 12.1.3. The **Add File Exception** help screen does not describe this new enhancement.
The location of the setting to automatically block an attacker's IP address is under Protection and Stealth (enterprise version) (3088214)	The section entitled "Automatically blocking connections to an attacking computer" incorrectly states the location of the setting to block an attacker's IP address. The correct location within the Firewall policy is under **Protection and Stealth**, under **Protection Settings**.
The help for directory authentication for an administrator account incorrectly states that you can leave the **Account Name** field blank (enterprise version) (2901470)	The online Help for the **Authentication** tab for adding an administrator account provides the following incorrect information: "You can leave **Account Name** blank so that the management server administrators are never locked out due to a password change on the directory server. You can use this anonymous directory authentication so that administrators can always log on to Symantec Endpoint Protection Manager." The help should say: "So that administrators are never locked out due to a password change on the directory server, create a directory server entry for anonymous access."

Table 1-2 Documentation and Help updates *(continued)*

Topic heading	Text change
The documentation for early launch anti-malware (ELAM) omits a reference (2969088)	References to ELAM in the documentation only mention Windows 8. The references should mention both Windows 8 and Windows Server 2012.
The documentation omits a reference for viewing or modifying the Windows ELAM settings (enterprise version) (3239019)	The section "Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options" does not mention that you can use the registry editor to view or modify ELAM settings.
The Symantec Endpoint Protection Manager help does not document an option for **Administrator Properties > Access Rights** (3107598)	The description for the **Remotely run commands** option should include the following statement: "You can also enable **Run commands on read-only groups** to let a limited administrator run a command on a group that the administrator cannot modify."
Trusted Web domain exceptions do not support HTTPS IP addresses (3107648)	The section "Excluding a trusted Web domain from scans" incorrectly states, "You must specify an HTTP or HTTPS URL or an IP address when you specify a trusted Web domain exception." This sentence should state, "You must specify an HTTP URL, an HTTP IP address, or an HTTPS URL when you specify a trusted Web domain exception." You cannot specify an HTTPS IP address.
The help incorrectly states that a check box for a notification condition still exists	In Symantec Endpoint Protection 11.0.7 (11.0 RU7) and later, the following notification option is no longer needed and was removed: **Include only clients which are currently online**. The help incorrectly states that this check box still exists. To view this option in earlier versions of the product, click **Monitors** > **Add Notification** > **Virus definitions out-of-date**.
The documentation incorrectly states that you can move a client between Symantec Endpoint Protection domains by replacing the Sylink.xml file (enterprise version) (3142416)	The section "About Domains" incorrectly states that you can copy clients between Symantec Endpoint Protection domains using the SylinkDrop tool. The client's domain setting in Symantec Endpoint Protection Manager overrides the client-side domain setting. This change in expected behavior was introduced in Symantec Endpoint Protection 12.1.2. To successfully move a client between domains, the administrator of the old domain must first delete the client from its group. When you then replace the communication settings file on the client, it should correctly check into the client group in the new domain.
The figures depicting the panels on the Enforcer appliance reflect an older model (3180356)	Two figures in the section "About the Enforcer appliance indicators and controls," which depict the panels on the Enforcer appliance, do not accurately reflect the current hardware. These figures also appear in the *Symantec Network Access Control 12.1.2 Getting Started Guide*.

Table 1-2 Documentation and Help updates *(continued)*

Topic heading	Text change

The documentation incorrectly states that the exported server properties file contains information about policies, group structure, and locations (enterprise version) (3150251)	The documentation contains incorrect information about policies in the following topics:
	■ "Exporting and importing server settings" should not say the following items:
	  ■ You upgrade the management server from a previous version to a newer version, and you need to import all the policies and locations.
	  ■ You want to export all policies rather than individual policies from one management server to another management server.
	  ■ The server properties file includes all policies, locations, and server settings.
	■ "Exporting and importing individual policies" should not say: "You export and import all policies by using the server properties file. The server properties file includes all policies, locations, and server settings. Symantec recommends that you use this method if you upgrade a legacy version of the management server to the current version of the management server."
	■ "What's new in Symantec Endpoint Protection 12.1.2" should not say: "You can export all the policies, locations, and server settings for a domain. If you then import these policies and settings into a new domain, you do not need to recreate them."
	■ "Performing the tasks that are common to all policies" should not say: "You can also export and import all policies rather than one policy at a time. If you upgrade the management server from a previous version to a newer version, you should export import all the policies."

The Symantec Endpoint Protection Manager help omits information about Private Insight Server (enterprise version) (3243915)	The help for **Admin > Servers > Local Site > Edit Site Properties > Private Insight Server** should include the following information in the description for the Server URL option: "If you change the Server URL to an invalid URL, clients use the previously valid URL. If the Server URL has never been configured and you enter an invalid URL, clients use the default Symantec Insight server."
Symantec Endpoint Protection and Symantec Network Access Control Client Guide lists incorrect Lotus Notes Auto-Protect version support (3259773)	The section "About the types of Auto-Protect" lists incorrect Lotus Notes versions for Auto-Protect support. Lotus Notes Auto-Protect supports Lotus Notes 7.x or later.
The Symantec Endpoint Protection Manager help displays incorrect restart delay information (2375361)	The help for **Admin > Install Packages > Client Install Settings > Add Client Install Settings...** displays incorrect information for a delayed restart. The user has five minutes to save unsaved data, not 60 seconds.

Table 1-2 Documentation and Help updates *(continued)*

Topic heading	Text change
The help in the Symantec Endpoint Protection Manager console and the Symantec Endpoint Protection client incorrectly states that the missed scheduled scan maximum retry interval for weekly scans is three days (2902211)	In the console, the help for **Virus and Spyware Protection Policy > Windows Settings > Scheduled Scans > Administrator-defined Scans > Scans > Add or Edit Scan > Schedule** is incorrect. In the client, the help for **Scan for Threats > Create a new scan – Schedule** is incorrect. The help for both areas should include the following revised statement: "If you set the frequency to Weekly, the maximum retry interval is seven days." The following sentence should also be added: "The defaults are the same as the maximums, except for weekly scans, which have a default of three days."
The Symantec Endpoint Protection Manager help for **Mac Auto-Protect: Scan Details** includes some incorrect information (3284773)	Under **General Scan Details**, the option **Do not scan** should be removed. Under **Scan Mounted Disk Details**, the option descriptions for **Scan disks when they are mounted**, **Show progress during scans of mounted disks**, and **Scan the following disks or devices** should be removed. The following text should be added: "You can choose to scan only data disks, all other disks and devices, or both. For legacy clients, you must configure separate options. The legacy client settings do not apply to 12.1.4 clients and later."
The documentation refers to an unsupported virtualization platform as supported (enterprise version) (3294038)	The section "Supported virtual installations and virtualization products" incorrectly lists Novell Xen as supported. The section also omits Citrix XenServer 5.6 or later as supported for Symantec Endpoint Protection 12.1.2 and later.
The documentation omits a reference about the version of Microsoft SQL Server Native Client (enterprise version) (3021590)	The section "About choosing a database type" omits information about which version of Microsoft SQL Server Native Client to install. For optimal compatibility, you install the version of SQL Server Native Client equal to your version of Microsoft SQL Server.

Supported upgrade paths for Symantec Endpoint Protection

The following Symantec Endpoint Protection Manager versions and Symantec Endpoint Protection Windows client versions can upgrade directly to version 12.1.4:

- From 11.x to 12.1.4 (enterprise version)
- 12.0.122.192 Small Business Edition
- 12.0.1001.95 Small Business Edition - Release Update 1 (RU1)
- 12.1.671.4971

- 12.1.1000.157 - Release Update 1 (RU1), with or without maintenance patches
- 12.1.2015.2015 - Release Update 2 (RU2), with or without maintenance patches
- 12.1.3001.165 - Release Update 3 (RU3)

For details on upgrading from specific versions of Symantec Endpoint Protection 11.x to 12.1, see the following knowledge base article:

Supported upgrade paths to Symantec Endpoint Protection Manager 12.1 from Symantec Endpoint Protection Manager 11.x

Symantec Endpoint Protection Manager and Symantec Endpoint Protection Windows client versions do not support the following downgrade paths:

- Symantec Endpoint Protection 11.x to 12.1.4 Small Business Edition
- Symantec Endpoint Protection 12.1.x (enterprise version) to 12.1.4 Small Business Edition

Symantec Endpoint Protection 12.1.4 supports a migration from Symantec AntiVirus 10.x, but does not support a migration from Symantec AntiVirus 9.x or Symantec Sygate Enterprise Protection 5.x.

For details on migrating from legacy products, see the following knowledge base article:

Migrating from Symantec AntiVirus or Symantec Client Security to Symantec Endpoint Protection 12.1 or later

The following Symantec Endpoint Protection Mac client versions can upgrade directly to version 12.1.4:

- From 11.x to 12.1.4
- 12.1.671.4971
- 12.1.1000.0157 - Release Update 1 (RU1)
- 12.1.2015.2015 - Release Update 2 (RU2)

You must uninstall Norton products before you install the Symantec Endpoint Protection Mac client. An installation of Symantec Endpoint Protection Mac over a Norton product is not supported.

Note: This release does not update the Symantec AntiVirus for Linux client, which remains version 1.0.14.

See "Supported and unsupported migration paths to Symantec Endpoint Protection" on page 17.

Supported and unsupported migration paths to Symantec Endpoint Protection

Symantec Endpoint Protection detects and migrates Symantec legacy virus protection software.

Table 1-3 Supported and unsupported migration paths

Product	Description
Symantec legacy virus protection software	You can migrate Symantec legacy virus protection software to Symantec Endpoint Protection. Migration detects and migrates installations of the following Symantec legacy virus protection software: ■ Symantec AntiVirus Corporate Edition 10.x ■ Symantec Client Security 3.x Migration from the following legacy products are not supported: ■ Symantec AntiVirus 9.x or earlier ■ Symantec Client Security 2.x ■ Symantec Sygate Enterprise Protection 5.x You may skip migration by using the following steps: 1 Uninstall the Symantec legacy virus protection software from your servers and client computers. 2 During Symantec Endpoint Protection Manager installation, do not select the migration option. 3 After initial product installation, use Symantec Endpoint Protection Manager to adjust the group settings and policy settings. 4 Install the Symantec Endpoint Protection client on the unprotected legacy computers.
Symantec Endpoint Protection	You can upgrade Symantec Endpoint Protection from Symantec Endpoint Protection 11.x or Small Business Edition 12.0, or to a new release update of 12.1. You can upgrade Symantec Endpoint Protection Small Business Edition from Symantec Endpoint Protection Small Business Edition 12.0, or to a new release update of 12.1. See "Supported upgrade paths for Symantec Endpoint Protection" on page 15.

System requirements for Symantec Endpoint Protection, Symantec Endpoint Protection Small Business Edition, or Symantec Network Access Control

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

Table 1-4 displays the minimum requirements for the Symantec Endpoint Protection Manager.

Table 1-5 displays the minimum requirements for the Symantec Endpoint Protection client.

Table 1-6 displays the minimum requirements for the Symantec Network Access Control client.

Table 1-7 displays the minimum requirements for the Symantec Network Access Control On-Demand client.

Table 1-4 Symantec Endpoint Protection Manager 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:** 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 may require additional RAM depending on the RAM requirements of other applications that are already installed.
Hard drive	Small Business Edition: 16 GB available minimum; 100 GB available recommended. Enterprise version: 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

Table 1-4 Symantec Endpoint Protection Manager system requirements *(continued)*

Component	Requirements
Operating system	■ Windows XP (32-bit, SP2 or later; 64-bit, all SPs; all editions except Home) ■ Windows 7 (32-bit, 64-bit; RTM and SP1; all editions except Home) ■ Windows 8 (32-bit, 64-bit; Windows To Go is not supported) ■ Windows 8.1 (32-bit, 64-bit) ■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit; R2, RTM, SP1 and SP2) ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows Small Business Server 2003 (32-bit) ■ Windows Small Business Server 2008 (64-bit) ■ Windows Small Business Server 2011 (64-bit) ■ Windows Essential Business Server 2008 (64-bit)
Web browser	■ Microsoft Internet Explorer 7, 8, 9, 10, 11 ■ Mozilla Firefox 3.6 through 24.0 ■ Google Chrome, through 30.0.1599.66 This list of supported browsers applies to the Symantec Endpoint Protection Manager only. For a list of supported browsers for Browser Intrusion Prevention, see the following webpage: Supported Browser versions for Browser Intrusion Prevention

Note: This Symantec Endpoint Protection Manager version can manage clients earlier than version 12.1, regardless of the client operating system.

Symantec Endpoint Protection Manager includes an embedded database. You may also choose to use one of the following versions of Microsoft SQL Server (enterprise version only):

- SQL Server 2005, SP4
- SQL Server 2008
- SQL Server 2008 R2
- SQL Server 2012

Table 1-5 Symantec Endpoint Protection Windows and Mac client system requirements

Component	Requirements
Processor	■ 32-bit processor for Windows: 1-GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended) ■ 64-bit processor for Windows: 2-GHz Pentium 4 with x86-64 support or equivalent minimum **Note:** Itanium processors are not supported. ■ 32-bit processor for Mac: Intel Core Solo, Intel Core Duo ■ 64-bit processor for Mac: Intel Core 2 Duo, Intel Quad-Core Xeon
Physical RAM	Windows: 512 MB of RAM (1 GB recommended), or higher if required by the operating system Mac: 2 GB of RAM
Hard drive	Windows: 850 MB 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. Mac: 500 MB of available hard disk space for the installation
Display	800 x 600
Operating system	■ Windows XP Home or Professional (32-bit, SP2 or later; 64-bit, all SPs) ■ Windows XP Embedded (SP2 and later) ■ Windows Vista (32-bit, 64-bit) ■ Windows 7 (32-bit, 64-bit; RTM and SP1) ■ Windows Embedded Standard 7 ■ Windows 8 (32-bit, 64-bit; Windows To Go is not supported) ■ Windows 8.1 (32-bit, 64-bit) ■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit; R2, SP1, and SP2) ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows Small Business Server 2003 (32-bit) ■ Windows Small Business Server 2008 (64-bit) ■ Windows Small Business Server 2011 (64-bit) ■ Windows Essential Business Server 2008 (64-bit) ■ Mac OS X 10.7, 10.8, 10.9

For information about the system requirements for the Symantec AntiVirus for Linux client, see the *Symantec AntiVirus for Linux Implementation Guide* or the following webpage:

System requirements for Symantec AntiVirus for Linux 1.0

Table 1-6 Symantec Network Access Control client system requirements

Component	Requirement
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.
Operating system	■ Windows XP (32-bit, SP2 or later; 64-bit, all SPs) ■ Windows XP Embedded ■ Windows Vista (32-bit, 64-bit) ■ Windows 7 (32-bit, 64-bit) ■ Windows 8 (32-bit, 64-bit) ■ Windows 8.1 (32-bit, 64-bit) ■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit) ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows Small Business Server 2008 (64-bit) ■ Windows Essential Business Server 2008 (64-bit)
Physical RAM	512 MB of RAM, or higher if required by the operating system
Hard disk	32-bit: 300 MB; 64-bit: 400 MB
Display	800 x 600

Table 1-7 Symantec Network Access Control On-Demand client system requirements

Component	Requirement
Processor	■ Windows: Intel Pentium II 550 MHz (1 GHz for Windows Vista) or faster ■ Mac: Intel CPU only

Table 1-7 Symantec Network Access Control On-Demand client system requirements *(continued)*

Component	Requirement
Operating system	■ Windows XP Home or Professional (32-bit; SP2 and SP3) ■ Windows Vista (32-bit, 64-bit) ■ Windows 7 (32-bit, 64-bit) ■ Windows 8 (32-bit, 64-bit) ■ Windows 8.1 (32-bit, 64-bit) ■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit; R2) ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows Small Business Server 2008 (64-bit) ■ Windows Essential Business Server 2008 (64-bit) ■ Mac OS X 10.5, 10.6 or 10.7
Disk space and physical RAM	■ Download size: 9 MB. The amount of free disk space that is needed to run the client: 100 MB. ■ Physical RAM for either Windows or Mac On-Demand client: 512 MB
Web browser	■ For Windows On-Demand Client: Microsoft Internet Explorer 6.0 or later; Mozilla Firefox 3.0 or later ■ For Mac On-Demand Client : Apple Safari 4.0 and 5.0; Mozilla Firefox 3.0 or later3 **Note:** All clients from version 11.0.6 (11.0 RU6) and earlier do not support a download by Firefox plug-in.
Other	■ Video display: Super VGA (1024 x 768) or higher ■ At least one Ethernet adapter (with TCP/IP installed)

For the most current system requirements, see the following webpage:

Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

Where to get more information about Symantec Endpoint Protection, Symantec Endpoint Protection Small Business Edition, and Symantec Network Access Control

The primary documentation is available in the Documentation folder on the Installation disc. For enterprise version users, tool-specific documents are located in the subfolders of the Tools disc.

This documentation is also available from the Symantec Technical Support website at the following locations:

- Symantec Endpoint Protection:
  Endpoint Protection
- Symantec Endpoint Protection Small Business Edition:
  Endpoint Protection Small Business Edition
- Symantec Network Access Control:
  Network Access Control

Each product includes the appropriate subset of the following documentation:

- *Symantec Endpoint Protection and Symantec Network Access Control Installation and Administration Guide*
- *Symantec Endpoint Protection Small Business Edition Installation and Administration Guide*
- *Symantec Endpoint Protection Getting Started Guide*
- *Symantec Endpoint Protection Small Business Edition Getting Started Guide*
- *Symantec Network Access Control Getting Started Guide*
- *Symantec Endpoint Protection and Symantec Network Access Control Client Guide*
- *Symantec Endpoint Protection Small Business Edition Client Guide*
- *Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper*
- *Symantec LiveUpdate Administrator User's Guide*
  This tool is located in the LiveUpdate folder on the Tools product disc.
- *Symantec Central Quarantine Implementation Guide*
  This tool is located in the CentralQ folder on the Tools product disc.
- *Symantec Endpoint Protection Manager Database Schema Reference*

Table 1-8 displays the websites where you can get additional information to help you use the product.

Table 1-8 Symantec websites

Types of information	Web address
Symantec Endpoint Protection trialware	http://www.symantec.com/business/products/downloads/
Public knowledge base Release details, updates, and patches Manuals and documentation updates Contact options	Symantec Endpoint Protection: http://www.symantec.com/business/support/overview.jsp?pid=54619 Symantec Endpoint Protection Small Business Edition: http://www.symantec.com/business/support/overview.jsp?pid=55357 Symantec Network Access Control: http://www.symantec.com/business/support/overview.jsp?pid=52788
Virus and other threat information and updates	http://www.symantec.com/business/security_response/index.jsp
Free online technical training	http://www.symantec.com/tv/search.jsp?q=endpoint+protection
Symantec Educational Services	http://www.symantec.com/theme.jsp?themeid=sep_training
Symantec Connect forums	Symantec Endpoint Protection: http://www.symantec.com/connect/security/forums/endpoint-protection-antivirus Symantec Endpoint Protection Small Business Edition: https://www-secure.symantec.com/connect/security/forums/endpoint-protection-small-business-edition-12x Symantec Network Access Control: http://www.symantec.com/connect/security/forums/network-access-control