Symantec™ Endpoint Protection, Symantec Endpoint Protection Small Business Edition, and Symantec Network Access Control 12.1.2 Release Notes

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

Product version: 12.1.2

Documentation version: 2

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Symantec Endpoint Protection 12.1.2 Release Notes

This document includes the following topics:

About this document

Review this document before you install or upgrade Symantec Endpoint Protection, Symantec Network Access Control, or Symantec Endpoint Protection Small Business Edition, or before you call for 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.

This document contains information for the following Symantec product editions:

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

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

What's new in Symantec Endpoint Protection 12.1.2

Table 1-1 describes the new features in the latest version of both Symantec Endpoint Protection (enterprise version) and Symantec Endpoint Protection Small Business Edition.

Table 1-2 describes additional new features in Symantec Endpoint Protection (enterprise version only).

Table 1-1 New features in Symantec Endpoint Protection and Symantec Endpoint Protection Small Business Edition 12.1.2

Feature	Description
System requirements	Symantec Endpoint Protection now supports additional new platforms and configurations. You can now install Symantec Endpoint Protection Manager on the following operating systems: ■ Windows 8 ■ Windows Server 2012 You can now install the Symantec Endpoint Protection client on the following operating systems: ■ Windows 8 and Windows Server 2012 ■ Mac OS X 10.8, Mountain Lion ■ Mac OS X case-sensitive formatted volumes You can now use Symantec Endpoint Protection Manager from the following browsers: ■ Microsoft Internet Explorer 10 ■ Google Chrome, through 22.0.1229.79 For the complete list of system requirements: See "System requirements for Symantec Endpoint Protection, Symantec Endpoint Protection Small Business Edition, or Symantec Network Access Control" on page 22. See the knowledge base article: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

Table 1-1 New features in Symantec Endpoint Protection and Symantec Endpoint Protection Small Business Edition 12.1.2 *(continued)*

Feature	Description
Installation	The Client Deployment Wizard includes the following changes: ■ The Client Deployment Wizard includes the **Communication Update Package Deployment** option to push the communications file (Sylink.xml) to the client in a client installation package. You use the Sylink.xml file to convert an unmanaged client to a managed client, or to manage a previously orphaned client. In previous releases, you needed to export the Sylink.xml file from the management server, and import Sylink.xml to each client. ■ The Client Deployment Wizard searches the network faster to find the computers that do not have the client software installed. ■ The Client Deployment Wizard includes the **Automatically uninstall existing security software** option so that a security software removal feature can uninstall third-party security products from the client computer. The feature removes security software before the client installation package installs the client software. With version 12.1.2, the feature removes more than 40 additional third-party products. For a list of products that the third-party security software removal feature uninstalls, see the knowledge base article: About the third-party security software removal feature in Symantec Endpoint Protection 12.1 You can download and run a new diagnostic tool on the management server and client to help you diagnose common issues before and after installation. The Symantec Help tool enables you to resolve product issues yourself instead of calling Support. See the knowledge base article at the following URL: Symantec Help
Remote management	Symantec Endpoint Protection provides public support to remotely manage and monitor the client and the management server. New Web services let you write your own tools to perform the following tasks remotely: ■ Run commands on the client to remediate threat situations. ■ Export policies from the server. ■ Apply policies to clients across servers. ■ Monitor license status and content status on the management server. Documentation and other tools for remote monitoring and management support appear in the Web services SDK, located in the following folder on the installation disc: `/Tools/Integration/SEPM_WebService_SDK`

Table 1-1 New features in Symantec Endpoint Protection and Symantec Endpoint Protection Small Business Edition 12.1.2 *(continued)*

Feature	Description
Windows 8 features	■ Support for the Microsoft Windows 8 style user interface, including toast notifications for critical events. ■ Support for Windows 8 and Windows Server 2012. ■ Windows 8 Early Launch Anti-Malware (ELAM) support provides a Microsoft-supported way for anti-malware software to start before all other third-party components. In addition, vendors can now control the launching of third-party drivers, depending on trust levels. If a driver is not trusted, it can be removed from the boot sequence. ELAM support makes more efficient rootkit detection possible.
Protection features	Virus and Spyware Protection: ■ Full support for the Microsoft Windows 8 style user interface. Exceptions: ■ Added support for HTTPS in trusted Web domain exceptions. ■ Common variables in exceptions now apply to 64-bit applications as well as 32-bit applications.
LiveUpdate	A link on the client **Status** page now lets end users quickly and easily confirm that the client has the most current content. The link displays the content version dialog box, where a new column lists the last time that the client checked each content type for updates. Users can be more confident that their client updates correctly and has the latest protection.

Table 1-2 Additional new features in Symantec Endpoint Protection 12.1.2 (enterprise version)

Feature	Description

Virtualization	Symantec Endpoint Protection includes the following virtualization improvements:
	■ A VMware vShield-enabled Shared Insight Cache. Delivered in a Security Virtual Appliance, you can deploy the vShield-enabled Shared Insight Cache into a VMware infrastructure on each host. The vShield-enabled Shared Insight Cache makes file scanning more efficient. You can monitor the Security Virtual Appliance and client status in Symantec Endpoint Protection Manager.
	■ For managing Guest Virtual Machines (GVMs) in non-persistent virtual desktop infrastructures:
	  ■ Symantec Endpoint Protection Manager includes a new option to configure the aging period for offline non-persistent GVMs. Symantec Endpoint Protection Manager removes the non-persistent GVM clients that have been offline longer than the specified time period.
	  ■ Symantec Endpoint Protection clients now have a configuration setting to indicate that they are non-persistent GVMs. You can filter out the offline non-persistent GVMs in the **Clients** tab view in Symantec Endpoint Protection Manager.

Table 1-2 Additional new features in Symantec Endpoint Protection 12.1.2 (enterprise version) *(continued)*

Feature	Description
Protection features	Proactive Threat Protection: ■ Device Control now sends a notification and creates a log event each time it blocks a previously disabled device. Previously, Device Control sent a notification and log event only the first time the device was disabled. ■ System lockdown can now run in blacklist mode. You must configure system lockdown to display a blacklist mode as well as the default whitelist mode. The blacklist mode blocks only the applications on the specified list. Symantec Endpoint Protection Manager can automatically update the existing file fingerprint lists and application name lists that system lockdown uses for whitelisting or blacklisting. Policies: ■ 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.
LiveUpdate	The LiveUpdate Settings policy includes an additional type of Group Update Provider (GUP) that allows clients to connect to Group Update Providers in a different subnet. This new type of GUP lets you explicitly define which networks each client may connect to. You can configure a single LiveUpdate policy to meet all your requirements.

See "What's new in Symantec Network Access Control 12.1.2" on page 10.

What's new in Symantec Network Access Control 12.1.2

Symantec Network Access Control 12.1.2 includes new features for Symantec Endpoint Protection Manager, Host Integrity policies, and the Enforcers.

Table 1-3 displays the new features for Host Integrity policies and the Enforcers.

Table 1-3 New features for Host Integrity policies and the Enforcers

Feature	Description
Host Integrity policies	The Symantec Endpoint Protection Manager Host Integrity policy includes the following new templates that you can import into a Host Integrity requirement. The Symantec Network Access Control client checks whether the client computer meets the requirements of the Host Integrity policy. To save time, you can create a Host Integrity requirement based on an existing template instead of creating a custom requirement. ■ **Removable Drive Scanning** The client scans USB drives after the drives are plugged in. The client then automatically scans the autorun.inf file and any file that is referenced in the autorun.inf file. ■ **Dual NIC Detection** The client checks whether the computer has dual NICs. If the computer has dual NICs, the client sets a registry key to use as a location switching criterion. The client can switch to a location to block the traffic, log the event, and send the end user a notification. ■ **Local GUP Status Detection** The client detects whether the local client is a Group Update Provider (GUP) client and checks whether the GUP works correctly. ■ **Check Domain Logon** The client checks whether the end user is logged on to the correct domain or workgroup. The client switches the end user to a different policy if the end user is not logged on to the correct domain. ■ **Check Wireless SSID** The client checks the SSID of a client computer to make sure that the computer is connected to the company's network. ■ **Disable Print Screen** The client disables the Windows Print Screen functionality. Because data in a picture is harder to detect than data in text, Print Screen captures represent a higher security risk. ■ **Check Security Center Status** The client checks the status of different security products that are configured through Windows Security Center. For example, the client can check whether an antivirus product is running and enabled or whether Windows Firewall is running and enabled.
Enforcers	■ Symantec Network Access Control can now quarantine an infected client. ■ The Enforcers now run on Red Hat Enterprise Linux 6.1. ■ The Enforcers include support for Enforcer Syslog events, which provides better monitoring. ■ You can assign a management server list to an Enforcer so that the Enforcer communicates to multiple management servers. ■ The Enforcers can now authenticate to servers in one management server list, but remain authorized to connect to servers in another management server list.

Known issues and workarounds

The issues in this section are new for Symantec Endpoint Protection version 12.1.2.

Please review this document in its entirety before you install Symantec Endpoint Protection, Symantec Network Access Control, Symantec Endpoint Protection Small Business Edition, or call for technical support. The release notes describe known issues and provide additional information that is not included in the standard documentation or the context-sensitive Help.

The known issues specific to the enterprise version and not the Small Business Edition display "enterprise version" at the end of the title. The known issues specific to Symantec Network Access Control appear in their own section.

- Known issues about upgrades, migration, and installation.
  See "Installation, upgrade, and migration issues" on page 12.
- Known issues that apply to the management server.
  See "Symantec Endpoint Protection Manager issues" on page 14.
- Known issues that apply to customizing policies.
  See "Symantec Endpoint Protection Manager policy issues" on page 15.
- Known issues that apply to virtualization.
  See "Virtualization issues" on page 15.
- Known issues that apply to the Windows client.
  See "Client issues" on page 16.
- Known issues that apply to Symantec Network Access Control only. These issues include issues related to the Enforcer and to Host Integrity policies.
  See "Symantec Network Access Control, Enforcers, and Host Integrity issues" on page 17.
- Known inaccurate information that is found only in the documentation for any one of the versions.
  See "Documentation and help issues" on page 17.

You can view a list of resolved issues and features at the following location:

New fixes and enhancements in Symantec Endpoint Protection 12.1 Release Update 2

Installation, upgrade, and migration issues

This section contains information about installation, upgrade, and migration issues.

Symantec Endpoint Protection 12.1.2 is not certified for FIPS 140-2 compliance (2710762)

Symantec Endpoint Protection 12.1.2 uses JRE 1.7 rather than JRE 1.6, as Oracle announced that public support for JRE 1.6 was due to end in November of 2012. Certified Crypto-J 6.0 and SSL-L J 6.0 libraries to support JRE 1.7 are not currently available from RSA. At the time of this publication, RSA has not yet released an official date by which these libraries will be certified. As a result, Symantec cannot certify the deployment of Symantec Endpoint Protection 12.1.2 in a FIPS-compliant configuration.

You cannot upgrade or migrate to 12.1.2 from a version of Symantec Endpoint Protection that has FIPS mode enabled. You must disable FIPS mode and return servers and clients to a non-FIPS state before you upgrade or migrate. FIPS mode does not exist in 12.1.2. To maintain FIPS-compliant protection, you should continue to use your current version of Symantec Endpoint Protection.

Symantec Endpoint Protection 12.1.2 does not support Windows To Go (2868431)

Symantec Endpoint Protection 12.1.2 does not support Windows To Go, an enterprise feature of Windows 8.

There is no workaround.

Management Server Configuration Wizard incorrectly indicates a migration path from Symantec Administration Console for Mac (2899897)

The Management Server Configuration Wizard erroneously displays some text that indicates that you can import policy and client configuration data from the Symantec Administration Console for Mac. Symantec Endpoint Protection 12.1.2 does not support this migration.

Unchecked setting "Delete clients that have not connected..." is checked after you upgrade (enterprise version only) (2941626)

After you upgrade to 12.1.2, the setting "Delete clients that have not connected..." is checked and set to the default of 30 days, even if you had previously unchecked it. You can uncheck it again under **Admin > Domains > Edit Domain Properties > General**.

Symantec Endpoint Protection Manager issues

This section contains information about Symantec Endpoint Protection Manager issues.

Symantec Endpoint Protection Manager now uses stronger encryption for remembering passwords and requires you to re-save legacy passwords (2739577)

Symantec Endpoint Protection Manager 12.1.2 uses AES encryption to store logon password credentials. A legacy Symantec Endpoint Protection Manager uses DES to store passwords. For security reasons, Symantec Endpoint Protection Manager 12.1.2 does not decrypt a DES password. The remember-me password is not backward-compatible. If you use the remember-me password option, a legacy DES password is intentionally not remembered when you upgrade to Symantec Endpoint Protection 12.1.2. After the upgrade, the password credential fields appear empty on the Symantec Endpoint Protection Manager logon screen. You must re-enter the password credentials to save the password with AES encryption.

The Chrome browser is incompatible with the help for Symantec Endpoint Protection Manager when launched through the Start menu (2853441)

For all parts of this release, you can view the help using Web browser. However, if Google Chrome is installed and is the default Web browser, you cannot open the help for Symantec Endpoint Protection Manager through the **Start** menu. Access to context-sensitive help from within Symantec Endpoint Protection Manager is not affected.

This issue applies to the help for all versions of the *Symantec Endpoint Protection and Symantec Network Access Control Installation and Administration Guide*, and for the *Integration Guide for Remote Monitoring and Management with Symantec Endpoint Protection*.

To work around this issue, you can open the help manually with Internet Explorer or Mozilla Firefox.

To manually open the help in Internet Explorer or Mozilla Firefox:

1. Navigate to *`installation_folder`*`\tomcat\webapps\ROOT\help\`.

   The default *installation_folder* is `C:\Program Files\Symantec\Symantec Endpoint Protection Manager` on 32-bit systems, or `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager` on 64-bit systems.

2. Right-click Spe.htm, click **Open With**, and then click **Internet Explorer** or **Mozilla Firefox**.

"Failed to validate certificate" message when you log on to Symantec Endpoint Protection Manager Web console (2918887)

You see a "failed to validate certificate" message when you log on to the Symantec Endpoint Protection Manager Web console. The Symantec Endpoint Protection Manager 12.1.2 uses a version of Java that no longer checks **Always trust content from this publisher** by default. To work around this message, you must now manually check this option when you log on.

The server logs show many SQL exception messages about SecurityAlertNotifyTask (2979245)

The message "java.sql.SQLException: Connection is closed," which references SecurityAlertNotifyTask, appears repeatedly in the `scm.server.log` on Symantec Endpoint Protection Manager. This message occurs because the connection is already closed and cannot be closed again. You can disregard these SecurityAlertNotifyTask messages.

Symantec Endpoint Protection Manager policy issues

This section includes information about working with policies in Symantec Endpoint Protection Manager.

Legacy clients do not honor the SONAR file exceptions set by Symantec Endpoint Protection Manager (2769428)

Symantec Endpoint Protection Manager 12.1.2 has added the capability to provide SONAR file path exceptions for specified applications. Legacy clients do not honor the SONAR exceptions that Symantec Endpoint Protection Manager 12.1.2 sets. You must upgrade those clients to 12.1.2. Similarly, a legacy Symantec Endpoint Protection Manager cannot provide SONAR exceptions to Symantec Endpoint Protection 12.1.2 clients.

Virtualization issues

This section contains information about virtualization issues.

Virtualization features support vSphere 5.1

Virtualization features in Symantec Endpoint Protection (enterprise version only) support the use of vSphere 5.1.

vSIC-enabled Windows 8 guest virtual machines are not supported (enterprise version only) (2833434)

Symantec Endpoint Protection 12.1.2 fully supports Windows 8 virtual machines. However, the use of vShield-enabled Shared Insight Cache (vSIC) for Windows 8 virtual machines is not supported.

Guest Virtual Machine client protection status in the Symantec Endpoint Protection Manager may change back and forth between unknown and protected (enterprise version only) (2630276)

Symantec Endpoint Protection Manager may temporarily report the Security Virtual Appliance status as unknown. This issue occurs when the guest virtual machines that it protects recover from sleep mode.

The number of clients reported with protected status in the Symantec Endpoint Protection Manager may differ from the number reported in the vShield Manager (enterprise version only) (2761305)

Because of reporting differences, the number of clients with protected status in the vShield Manager may differ from the number with protected status in Symantec Endpoint Protection Manager.

There is no workaround. As a best practice, Symantec recommends that you monitor client protection status in the Symantec Endpoint Protection Manager rather than in vShield Manager.

Client issues

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

Tamper Protection default settings on the client have changed to Block and do not log (2893286)

By default, Tamper Protection is now set to **Block and do not log**. The new default setting applies to new installations. Upgrades to existing installations retain their current settings. The new default setting prevents Tamper Protection from generating a large number of log events.

Also, you can no longer configure notifications for Tamper Protection.

Configuring an NTLM-enabled proxy to be used with HTTP basic authentication causes client LiveUpdate to return an error on the clients that run Windows XP/Vista (2750314)

Windows XP/Vista removes the authentication credentials that are submitted when you configure Symantec Endpoint Protection to use an NTLM-enabled proxy with basic authentication on the HTTP(S) host. This removal causes the client's LiveUpdate to return an error message.

There is no workaround.

Symantec Network Access Control, Enforcers, and Host Integrity issues

The issues listed in the following section relate to Symantec Network Access Control, Enforcers, and Host Integrity.

LAN and Gateway Enforcers cannot apply Enforcer profiles larger than 32 MB (2781335)

The Enforcer profiles for the LAN Enforcer and the Gateway Enforcer cannot exceed 32 MB.

There is no workaround.

The Host Integrity policy custom requirement for running a Symantec antivirus check does not work on releases of Symantec Network Access Control prior to 12.1.2 (2692623)

The Host Integrity custom requirement for running a Symantec antivirus check is new in Symantec Network Access Control 12.1.2, and does not work on previous releases of Symantec Network Access Control.

Documentation and help issues

This section describes issues in the documentation and context-sensitive help.

A change in a client group no longer triggers a notification (2915552)

In the section "What are the types of notifications and when are they sent?", the description for "Client list changed" contains erroneous information. A change in a client group no longer triggers a notification.

This section 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.

The Symantec Diagnostic and Product Advisor is now named Symantec Help

The localized documentation for the Symantec Endpoint Protection 12.1.2 release includes some references to a new troubleshooting tool that is called the Symantec Diagnostic and Product Advisor. Symantec has since renamed this tool to Symantec Help, or SymHelp.

Help documentation for the Symantec Endpoint Protection client 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.

Supported and unsupported migration paths to Symantec Endpoint Protection

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

Table 1-4 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 ■ Symantec AntiVirus for Mac (client only) 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 as follows: ■ Uninstall the Symantec legacy virus protection software from your servers and client computers. ■ During Symantec Endpoint Protection Manager installation, do not select the migration option. ■ After initial product installation, use Symantec Endpoint Protection Manager to adjust the group settings and policy settings. ■ Install the Symantec Endpoint Protection client on the unprotected legacy computers. See "Supported migration paths for the Symantec Endpoint Protection Mac client" on page 21.
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 from Symantec Endpoint Protection Small Business Edition 12.0, or to a new release update of 12.1. See "Supported upgrade paths for the Symantec Endpoint Protection client" on page 20.

Supported upgrade paths for Symantec Endpoint Protection Manager

The following Symantec Endpoint Protection Manager upgrade paths are supported:

- From 11.x to 12.1.2 (enterprise version)
- From 12.0 Small Business Edition to 12.1.2 (enterprise version)
- From 12.0 Small Business Edition to 12.1.2 Small Business Edition
- From 12.1 Small Business Edition to 12.1.2 Small Business Edition
- From 12.1 Small Business Edition to 12.1.2 (enterprise version)
- From 12.1 (enterprise version) to 12.1.2 (enterprise version)

Note: Symantec AntiVirus 10.x server information can be imported during the installation of Symantec Endpoint Protection Manager version 12.1.2.

The following downgrade paths are not supported:

- Symantec Endpoint Protection 11.x to 12.1.2 Small Business Edition
- 12.1.x (enterprise version) to 12.1.2 Small Business Edition

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

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

Supported upgrade paths for the Symantec Endpoint Protection client

The following Symantec Endpoint Protection Windows client versions can upgrade directly to version 12.1.2:

- 11.0.780.1109
- 11.0.1000.1375 - Maintenance Release 1 (MR1)
- 11.0.2000.1567 - Maintenance Release 2 (MR2), with or without maintenance patches
- 11.0.3001.2224 - Maintenance Release 3 (MR3)

- 11.0.4000.2295 - Maintenance Release 4 (MR4), with or without maintenance patches
- 11.0.5002.333 - Release Update 5 (RU5)
- 11.0.6000.550 - Release Update 6 (RU6), with or without maintenance patches
- 11.0.7000.975 - Release Update 7 (RU7), with or without maintenance patches
- 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

The following downgrade paths for Windows clients are not supported:

- Symantec Endpoint Protection 11.x to 12.1 Small Business Edition
- 12.1.x (enterprise version) to 12.1.2 Small Business Edition

The following Symantec Endpoint Protection Mac client versions can upgrade directly to version 12.1.2:

- 11.0.6000 (0162) - Release Update 6 (RU6), with or without maintenance patches
- 11.0.7000 (0217) - Release Update 7 (RU7), with or without maintenance patches
- 12.1.671.4971
- 12.1.1000.0157 - Release Update 1 (RU1)

Migrating from Symantec AntiVirus 10.x to 12.1 is supported. Migrating from Symantec AntiVirus 9.x and Symantec Sygate Enterprise Protection 5.x is not supported.

See "Supported migration paths for the Symantec Endpoint Protection Mac client" on page 21.

See "Supported and unsupported migration paths to Symantec Endpoint Protection" on page 18.

Supported migration paths for the Symantec Endpoint Protection Mac client

Table 1-5 displays the products that can be migrated to the Symantec Endpoint Protection Mac client.

Table 1-5 Migration paths from Symantec AntiVirus for Mac to the Symantec Endpoint Protection Mac client

Migrate from	Migrate to	Supported?
Managed Symantec AntiVirus for Mac client	Managed Symantec Endpoint Protection for Mac client	Yes
Unmanaged Symantec AntiVirus for Mac client	Unmanaged Symantec Endpoint Protection for Mac client	Yes
Unmanaged Symantec AntiVirus for Mac client	Managed Symantec Endpoint Protection for Mac client	Yes
Managed Symantec AntiVirus for Mac client	Unmanaged Symantec Endpoint Protection for Mac client	Yes, but managed client settings are retained.
Norton AntiVirus for Mac	Managed or unmanaged Symantec Endpoint Protection for Mac client	No. Client must uninstall Norton products before installing Symantec Endpoint Protection.

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 1-6 displays the minimum requirements for the Symantec Endpoint Protection Manager.

Table 1-7 displays the minimum requirements for the Symantec Endpoint Protection client.

Table 1-8 displays the minimum requirements for the Symantec Network Access Control client.

Table 1-9 displays the minimum requirements for the Symantec Network Access Control On-Demand client.

Table 1-6 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	1 GB of RAM for 32-bit operating systems, 2 GB of RAM for 64-bit operating systems, or higher if required by the operating system
Hard drive	4 GB or more free space; plus 4 GB for the locally installed database.
Display	1024 x 768
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 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 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 ■ Mozilla Firefox 3.6 through 15.0.1 ■ Google Chrome, through 22.0.1229.79

Note: This version of the Symantec Endpoint Protection Manager can manage clients before 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

Note: If you install the Symantec Endpoint Protection Manager and the SQL database on the same computer, a minimum of 4 GB of RAM is recommended.

Table 1-7 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) ■ 32-bit processor for Mac: Intel Core Solo, Intel Core Duo. PowerPC processors are not supported. ■ 64-bit processor for Windows: 2-GHz Pentium 4 with x86-64 support or equivalent minimum. Itanium processors are not supported. ■ 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: 1 GB of RAM for 10.6; 2 GB for 10.7 and 10.8
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

Table 1-7 Symantec Endpoint Protection Windows and Mac client system requirements *(continued)*

Component	Requirements
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 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 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 10.6.8, 10.7 (32-bit, 64-bit); 10.8 (64-bit) ■ Mac OS X Server 10.6.8, 10.7 (32-bit, 64-bit); 10.8 (64-bit)

For information about the system requirements for the Symantec AntiVirus client on Linux, see the *Symantec AntiVirus for Linux Implementation Guide*.

Table 1-8 Symantec Network Access Control client system requirements

Component	Requirement
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. Itanium processors are not supported.

Table 1-8 Symantec Network Access Control client system requirements *(continued)*

Component	Requirement
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 Server 2003 (32-bit, 64-bit, R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit) ■ Windows Server 2012 ■ 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 1-9 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
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 Server 2003 (32-bit, 64-bit, R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit, R2) ■ Windows Server 2012 ■ Windows Small Business Server 2008 (64-bit) ■ Windows Essential Business Server 2008 (64-bit) ■ Mac OS X 10.5, 10.6 or 10.7

Table 1-9 Symantec Network Access Control On-Demand client system requirements *(continued)*

Component	Requirement
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 2.0, 3.0, 3.5, 3.6.3, 11.0 **Note:** Clients from version 11.0 RU6 and lower do not support Firefox 3.6.3. ■ For Mac On-Demand Client : Apple Safari 4.0 and 5.0; Mozilla Firefox 2.0, 3.0, 3.5, 3.6.3 **Note:** Clients from version 11.0 RU6 and lower do not support Firefox 3.6.3.
Other	■ Video display: Super VGA (1,024 x 768) or higher ■ At least one Ethernet adapter (with TCP/IP installed)

For the most current system requirements, see: 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 product disc. Tool-specific documents are located in the subfolders of the Tools folder on the Tools product disc.

Updates to the documentation are available from the Symantec Technical Support Web site at the following location:

- Symantec Endpoint Protection:
  Endpoint Protection
- Symantec Endpoint Protection Small Business Edition:
  Endpoint Protection Small Business Edition

- Symantec Network Access Control:
  Network Access Control

The product includes the following documentation:

- *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 Installation and Administration Guide*
- *Symantec Endpoint Protection Small Business Edition Installation and Administration Guide*
- *Symantec Endpoint Protection and Symantec Network Access Control Client Guide*
- *Symantec Endpoint Protection Small Business Edition Client Guide*
- *Symantec LiveUpdate Administrator User's Guide*
  This tool is located in the Tools\LiveUpdate folder on the Tools product disc.
- *Symantec Central Quarantine Implementation Guide*
  This tool is located in the Tools\CentralQ folder on the Tools product disc.
- *Symantec Endpoint Protection Manager Database Schema Reference*
  This document is located on the Symantec Technical Support Web site:
  Endpoint Protection

Table 1-10 displays the Web sites where you can get additional information to help you use the product.

Table 1-10 Symantec Web sites

Types of information	Web address
Symantec Endpoint Protection software	http://www.symantec.com/business/products/downloads/
Public knowledge base Releases and updates 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

Table 1-10 Symantec Web sites *(continued)*

Types of information	Web address
Virus and other threat information and updates	http://www.symantec.com/business/security_response/index.jsp
Product news and updates	http://enterprisesecurity.symantec.com
Free online technical training	http://go.symantec.com/education_septc
Symantec Educational Services	http://go.symantec.com/education_sep
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