Symantec™ Endpoint Protection, Symantec Endpoint Protection Small Business Edition, and Symantec Network Access Control 12.1.3 Release Notes

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

Product version: 12.1.3

Documentation version: 1

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Release notes

This document includes the following topics:

About this document

This document contains information for the following Symantec 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.

What's new in Symantec Endpoint Protection 12.1.3 (12.1 RU3)

This release contains the following new features:

Table 1-1 New features for 12.1.3

Feature	Benefit
Support for Microsoft Outlook 2013	The Microsoft Outlook Auto-Protect plug-in adds support for Microsoft Outlook 2013.
Support for Microsoft Exchange 2013 Server	Symantec Endpoint Protection now detects the default installation of Microsoft Exchange 2013 Server and automatically excludes Microsoft Exchange files and folders.
Intelligent Updater support for Proactive Threat Protection and Network Threat Protection	Added support for Intelligent Updater to provide content for Proactive Threat Protection and Network Threat Protection. You can download this content for Symantec Endpoint Protection 12.1.3 from the Symantec Security Response website: http://www.symantec.com/security_response/definitions.jsp
FIPS 140-2 certification	You can deploy Symantec Endpoint Protection with a FIPS-compliant configuration to protect its server-to-server and client-to-server communications.

Known issues and workarounds

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

Note: The issues in this section that are labeled as version 12.1.2 also apply to version 12.1.3.

The known issues specific to the enterprise version and not the Small Business Edition display "enterprise version" at the end of the topic 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 7.
- Known issues about the management server.
  See "Symantec Endpoint Protection Manager issues" on page 8.
- Known issues about customizing policies.
  See "Symantec Endpoint Protection Manager policy issues" on page 9.
- Known issues about virtualization.
  See "Virtualization issues" on page 9.
- Known issues about the Windows 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.
- Known inaccurate information that is found only in the documentation for any one of the versions.
  See "Documentation and help issues" on page 11.

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

New fixes and enhancements in Symantec Endpoint Protection 12.1 Release Update 3 (12.1 RU3)

Installation, upgrade, and migration issues

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

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.

Unchecked setting "Delete clients that have not connected..." is checked after you upgrade (enterprise version) (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 by clicking **Admin > Domains > Edit Domain Properties > General**.

Symantec Endpoint Protection Manager issues

This section contains information about Symantec Endpoint Protection Manager.

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

For this release, you can view the help using a 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. This issue does not affect access to context-sensitive Help from within Symantec Endpoint Protection Manager.

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 appears 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 Symantec Endpoint Protection Manager console user interface for early launch anti-malware (ELAM) omits a reference (2969088)

User interface text for the ELAM feature in the Symantec Endpoint Protection Manager console refers only to Windows 8. The user interface text should appear as **Windows 8 and Windows Server 2012**.

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.

Virtualization features support vSphere 5.1 (enterprise version)

Virtualization features in Symantec Endpoint Protection support vSphere 5.1.

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

The Symantec Endpoint Protection client must be the same version as the Virtual Image Exception tool (enterprise version) (3020699)

The VIETool.exe crashes if it is not the same version as the installed client. The client must be the same version as the Virtual Image Exception tool.

Client issues

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

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 LiveUpdate to return an error message.

There is no workaround.

The Symantec Endpoint Protection client user interface for early launch anti-malware (ELAM) omits a reference (2969088)

User interface text for the ELAM feature in the Symantec Endpoint Protection client refers only to Windows 8. The user interface text should appear as "Windows 8 and Windows Server 2012."

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 earlier than 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 in earlier releases of Symantec Network Access Control.

Documentation and help issues

This section describes documentation issues in the PDFs and the online Help. Unless otherwise specified, the issue occurs 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 fixes these issues on the Support page, but not in the PDFs or online Help until the next major release.

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 Symantec Endpoint Protection 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 to Symantec Endpoint Protection 12.1.3. The **Add File Exception** Help screen does not describe this new enhancement.

"Automatically block an attacker's IP address" is located 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**.

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."

User documentation for early launch anti-malware (ELAM) omits a reference (2969088)

References to ELAM in the documentation only mention Windows 8. The references should be "Windows 8 and Windows Server 2012."

These references also appear in *Symantec Endpoint Protection and Symantec Network Access Control Client Guide*, the *Symantec Endpoint Protection Small Business Edition Client Guide*, and the context-sensitive Help for the Symantec Endpoint Protection client.

Help does not document the option "Run commands on read-only groups" when you create a limited administrator (3107598)

The online Help does not document a new feature to Symantec Endpoint Protection 12.1.3, which grants limited administrators the ability to remotely run commands on read-only groups. You can access the Symantec Endpoint Protection Manager Help page **Administrator Properties: Access Rights** through the **Add Administrator** dialog box.

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.

Help documentation incorrectly states that a check box for a notification condition still exists

In Symantec Endpoint Protection version 11 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**.

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*.

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."

Supported upgrade paths for Symantec Endpoint Protection

The following Symantec Endpoint Protection Manager versions and Symantec Endpoint Protection client versions for Windows can upgrade directly to version 12.1.3:

- From 11.x to 12.1.3 (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

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

The following downgrade paths for Symantec Endpoint Protection Manager and Symantec Endpoint Protection client versions for Windows are not supported:

- Symantec Endpoint Protection 11.x to 12.1.3 Small Business Edition
- 12.1.x (enterprise version) to 12.1.3 Small Business Edition

---

Note: This release does not update the Symantec Endpoint Protection Mac client, which remains version 12.1.2. This release also does not update the Symantec Antivirus for Linux client, which remains version 1.0.14.

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.

For details on migrating from legacy products, see:

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

See "Supported and unsupported migration paths to Symantec Endpoint Protection" on page 16.

See "Supported migration paths to the Symantec Endpoint Protection Mac client" on page 18.

Supported and unsupported migration paths to Symantec Endpoint Protection

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

Table 1-2 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 to the Symantec Endpoint Protection Mac client" on page 18.
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 Symantec Endpoint Protection" on page 15.

Supported migration paths to the Symantec Endpoint Protection Mac client

Table 1-3 displays the products that can be migrated to the Symantec Endpoint Protection Mac client.

Table 1-3 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 1-4 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 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
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)

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

Component	Requirements
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

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) ■ 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 OS X 10.6; 2 GB for OS X 10.7 and 10.8

Table 1-5 Symantec Endpoint Protection Windows and Mac client system requirements *(continued)*

Component	Requirements
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 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

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

Table 1-6 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 1-6 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 1-7 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
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 1-7 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 11.0.6 (11.0 RU6) and earlier 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 11.0.6 (11.0 RU6) and earlier 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 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

Table 1-8 Symantec websites *(continued)*

Types of information	Web address
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