Symantec™ Endpoint Protection 12.1.2 Getting Started Guide

Symantec Endpoint Protection Getting Started Guide

Product version: 12.1.2

Documentation version: 1

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Getting Started with Symantec Endpoint Protection

This document includes the following topics:

About Symantec Endpoint Protection

Symantec Endpoint Protection is a client-server solution that protects laptops, desktops, Windows and Mac computers, and servers in your network against

malware. Symantec Endpoint Protection combines virus protection with advanced threat protection to proactively secure your computers against known and unknown threats.

Symantec Endpoint Protection protects against malware such as viruses, worms, Trojan horses, spyware, and adware. It provides protection against even the most sophisticated attacks that evade traditional security measures, such as rootkits, zero-day attacks, and spyware that mutates. Providing low maintenance and high power, Symantec Endpoint Protection communicates over your network to automatically safeguard for both physical systems and virtual systems against attacks.

This comprehensive solution protects confidential and valuable information by combining multiple layers of protection on a single integrated client. Symantec Endpoint Protection reduces management overhead, time, and cost by offering a single management console for clients.

See "About the types of threat protection that Symantec Endpoint Protection provides" on page 7.

What's new in Symantec Endpoint Protection 12.1.2

Table 1-1 describes the new features in the latest version of Symantec Endpoint Protection.

Table 1-1 New features in Symantec Endpoint Protection 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 For the complete list of system requirements: See "System requirements for Symantec Endpoint Protection" on page 18. See the knowledge base article: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control
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 See "Deploying clients using a Web link and email" on page 25. 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 (SymHelp)

Table 1-1 New features in Symantec Endpoint Protection 12.1.2 *(continued)*

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.
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`
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.

Table 1-1 New features in Symantec Endpoint Protection 12.1.2 *(continued)*

Feature	Description
Protection features	Virus and Spyware Protection: ■ Full support for the Microsoft Windows 8 style user interface. 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. 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. 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. 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.

About the types of threat protection that Symantec Endpoint Protection provides

You need combinations of all the protection technologies to fully protect and customize the security in your environment. Symantec Endpoint Protection combines traditional scanning, behavioral analysis, intrusion prevention, and community intelligence into a superior security system.

Table 1-2 describes the types of protection that the product provides and their benefits.

Table 1-2 Layers of protection

Protection type	Description	Benefit
Virus and Spyware Protection	Virus and Spyware Protection protects computers from viruses and security risks, and in many cases can repair their side effects. The protection includes real-time scanning of files and email as well as scheduled scans and on-demand scans. Virus and spyware scans detect viruses and the security risks that can put a computer, as well as a network, at risk. Security risks include spyware, adware, and other malicious files.	Virus and Spyware Protection detects new threats earlier and more accurately using not just signature-based and behavioral-based solutions, but other technologies as well. ■ Symantec Insight provides faster and more accurate malware detection to find the new and the unknown threats that other approaches miss. Insight identifies new and zero-day threats by using the collective wisdom of millions of systems in hundreds of countries. ■ Bloodhound uses heuristics to detect known and unknown threats. ■ Auto-Protect scans files from a signature list as they are read from or written to the client computer.
Network Threat Protection	Network Threat Protection provides a firewall and an intrusion prevention system to prevent intrusion attacks and malicious content from reaching the computer that runs the client software. The firewall allows or blocks network traffic based on the various criteria that the administrator sets. If the administrator permits it, end users can also configure firewall policies. The Intrusion Prevention System (IPS) analyzes all the incoming and the outgoing information for the data patterns that are typical of an attack. It detects and blocks malicious traffic and attempts by outside users to attack the client computer. Intrusion prevention also monitors outbound traffic and prevents the spread of worms.	■ The rules-based firewall engine blocks malicious threats before they can harm the computer. ■ The IPS scans network traffic and files for indications of intrusions or attempted intrusions. ■ Browser Intrusion Prevention scans for the attacks that are directed at browser vulnerabilities. ■ Universal download protection monitors all downloads from browsers and validates that the downloads are not malware.

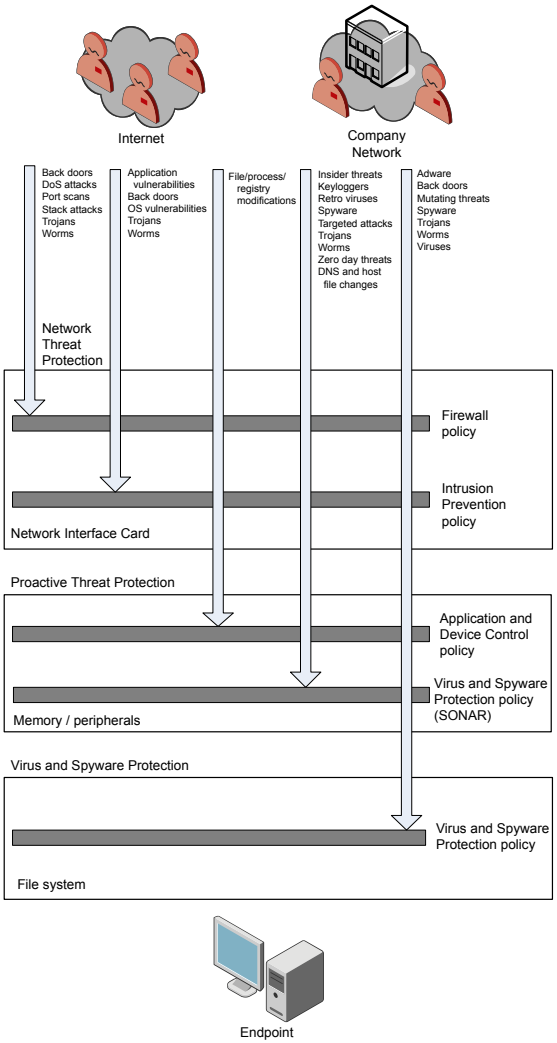
Table 1-2 Layers of protection *(continued)*

Protection type	Description	Benefit
Proactive Threat Protection	Proactive Threat Protection uses SONAR to protect against zero-day attack vulnerabilities in your network. Zero-day attack vulnerabilities are the new vulnerabilities that are not yet publicly known. Threats that exploit these vulnerabilities can evade signature-based detection, such as spyware definitions. Zero-day attacks may be used in targeted attacks and in the propagation of malicious code. SONAR provides real-time behavioral protection by monitoring processes and threats as they execute. Application and Device Control monitors and controls the behavior of applications on client computers and manages the hardware devices that access client computers.	SONAR examines programs as they run, and identifies and stops malicious behavior of new and previously unknown threats. SONAR uses heuristics as well as reputation data to detect emerging and unknown threats. Application Control controls what applications are allowed to run or access system resources. Device Control manages the peripheral devices that users can attach to desktop computers.

The management server enforces each protection by using an associated policy that is downloaded to the client.

Figure 1-1 shows the categories of threats that each type of protection blocks.

Figure 1-1 An overview of protection layers



Components of Symantec Endpoint Protection

Table 1-3 lists the product's components and describes their functions.

Table 1-3 Product components

Component	Description
Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager is a management server that manages the client computers that connect to your company's network. Symantec Endpoint Protection Manager includes the following components: ■ The management server software provides secure communication to and from the client computers and the console. ■ The console is the interface to the management server. The console software coordinates and manages security policies, client computers, reports, logs, roles and access, administrative functions, and security. You can also install a remote console and use it to log on to the management server from any computer with a network connection. See "Installing Symantec Endpoint Protection Manager" on page 20.
Database	The database stores security policies and events. You install the embedded database on the computer that hosts Symantec Endpoint Protection Manager. You can also separately install the Microsoft SQL Server database to use instead of the embedded database.
Symantec Endpoint Protection client	The client protects computers with virus and spyware scans, SONAR, Download Insight, a firewall, an intrusion prevention system, and other protection technologies. It runs on the servers, desktops, and portable computers that you want to protect. The Symantec Endpoint Protection Mac client protects the computers with virus and spyware scans. For more information about using the client, see the *Symantec Endpoint Protection and Symantec Network Access Control Client Guide*. See "About Symantec Endpoint Protection" on page 3.
Symantec Protection Center (optional)	Symantec Protection Center lets you integrate management consoles from multiple supported Symantec security products into a single management environment. Symantec Endpoint Protection integrates with Protection Center by means of a series of Web services. You download and install Protection Center version 2 separately. See the Symantec Protection Center 2.0 Getting Started Guide
LiveUpdate Administrator (optional)	The LiveUpdate Administrator downloads definitions, signatures, and product updates from a Symantec LiveUpdate server and distributes the updates to client computers. For more information, see the *Symantec LiveUpdate Administrator User's Guide*.

Table 1-3 Product components *(continued)*

Component	Description
Central Quarantine (optional)	The Central Quarantine receives suspicious files and unrepaired infected items from the Symantec Endpoint Protection clients. Central Quarantine forwards a sample to Symantec Security Response, which analyzes the sample. If a threat is new, Symantec Security Response produces security updates. For more information, see the *Symantec Central Quarantine Implementation Guide*.

For more information, see the *Symantec Endpoint Protection and Symantec Network Access Control Installation and Administration Guide*.

See "About the types of threat protection that Symantec Endpoint Protection provides" on page 7.

Getting up and running on Symantec Endpoint Protection for the first time

You should assess your security requirements and decide if the default settings provide the balance of performance and security that you require. Some performance enhancements can be made immediately after you install Symantec Endpoint Protection Manager.

Table 1-4 lists the tasks that you should perform to install and protect the computers in your network immediately.

Table 1-4 Tasks to install and configure Symantec Endpoint Protection

Action	Description
Plan your network architecture	Before you install the product, perform the following tasks: ■ Make sure the computer on which you install the management server meets the minimum system requirements. For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control ■ If you install or upgrade to the Microsoft SQL Server database, make sure that you have the user name and password information. ■ For networks with more than 500 clients, determine the sizing requirements. For more information to help you plan medium to large-scale installations, see the Symantec white paper, Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper.

Table 1-4 Tasks to install and configure Symantec Endpoint Protection *(continued)*

Action	Description
Install, upgrade, or migrate the management server	Whether you install the product for the first time, upgrade from a previous version, or migrate from another product, you install Symantec Endpoint Protection Manager first. See "Installing Symantec Endpoint Protection Manager" on page 20.
Create groups and locations	You can add groups that contain computers based on the level of security or function the computers perform. For example, you should put computers with a higher level of security in one group, or a group of Mac computers in another group. You can use the following group structure as a basis: ■ Desktops ■ Laptops ■ Servers You can migrate existing Active Directory groups when you install Symantec Endpoint Protection Manager. If you are running legacy Symantec protection, you usually upgrade policy and group settings from your older version. You can apply a different level of security to computers based on whether they are inside or outside the company network. To use this method, you create separate locations and apply different security policies to each location. In general, the computers that connect to your network from outside of your firewall need to have stronger security than those that are inside your firewall. You can set up a location that allows the mobile computers that are not in the office to update their definitions automatically from Symantec's LiveUpdate servers.
Disable inheritance on special groups	By default, groups inherit the security and the policy settings from the default parent group, **My Company**. You must disable inheritance before you can change the policy settings for any new groups that you create.

Table 1-4 Tasks to install and configure Symantec Endpoint Protection *(continued)*

Action	Description
Change communication settings to increase performance	You can improve network performance by modifying the following client-server communication settings in each group: ■ Use pull mode instead of push mode to control when clients use network resources to download policies and content updates. ■ Increase the heartbeat interval and the randomization interval. For under 100 clients per server, increase the heartbeat to 15-30 minutes. For 100 to 1,000 clients, increase the heartbeat to 30-60 minutes. Larger environments might need a longer heartbeat interval. ■ Increase the download randomization to between one and three times the heartbeat interval. For more information, see the Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper.
Activate the product license	Purchase and activate a license within 60 days of product installation. See "Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license" on page 22.
Prepare computers for remote client installation (optional)	If you deploy client software remotely, first modify the firewall settings on your client computers to allow communication between the computers and the management server.
Install the client software by using the Client Deployment Wizard	Create a client installation package and deploy it on your client computers. See "Deploying clients using a Web link and email" on page 25. Create a custom client install feature set with the following settings: ■ Use **Computer mode** for most environments, not **User mode**. ■ For client installation packages for workstations, check the email scanner protection option that applies to the mail server in your environment. For example, if you use a Microsoft Exchange mail server, check **Microsoft Outlook Scanner**.

Table 1-4 Tasks to install and configure Symantec Endpoint Protection *(continued)*

Action	Description
Check that the computers are listed in the groups that you expected and that the clients communicate with the management server	In the management console, on the **Clients** > **Clients** page: 1 Change the view to **Client status** to make sure that the client computers in each group communicate with the management server. Look at the information in the following columns: ■ The **Name** column displays a green dot for the clients that are connected to the management server. ■ The **Last Time Status Changed** column displays the time that each client last communicated with the management server. ■ The **Restart Required** column displays the client computers you need to restart to enable protection. ■ The **Policy Serial Number** column displays the most current policy serial number. The policy might not update for one to two heartbeats. You can manually update the policy on the client if the policy does not update immediately. 2 Change to the **Protection technology** view and ensure that the status is set to **On** in the columns between and including **AntiVirus Status** and **Tamper Protection Status**. 3 On the client, check that the client is connected to a server, and check that the policy serial number is the most current one.

Table 1-5 displays the tasks to perform after you install and configure the product to assess whether the client computers have the correct level of protection.

Table 1-5 Tasks to perform two weeks after you install

Action	Description
Modify the Virus and Spyware Protection policy	Change the following default scan settings: ■ If you create a group for servers, change the scheduled scan time to a time when most users are offline. ■ Enable Risk Tracer in Auto-Protect. For more information, see the Symantec Technical Support knowledge base article, What is Risk Tracer? Risk Tracer has the following prerequisites: ■ Network Threat Protection is enabled. ■ Windows File and Printer Sharing is turned on.

Table 1-5 Tasks to perform two weeks after you install *(continued)*

Action	Description
Modify the Firewall policy for the remote computers group and the servers group	■ Increase the security for remote computers by making sure that the following default firewall rules for an off-site location are enabled: ■ **Block Local File Sharing to external computers** ■ **Block Remote Administration** ■ Decrease the security for the servers group by making sure that the following firewall rule is enabled: **Allow Local File Sharing to local computers**. This firewall rule ensures that only local traffic is allowed.
Exclude applications and files from being scanned	You can increase performance by configuring the client not to scan certain folders and files. For example, the client scans the mail server directory every time a scheduled scan runs. You should exclude mail server program files and directories from being scanned. For more information, see the knowledge base article: About the automatic exclusion of files and folders for Microsoft Exchange server and Symantec products. You can improve performance by excluding the folders and files that are known to cause problems if they are scanned. For example, Symantec Endpoint Protection should not scan the proprietary Microsoft SQL Server files. You should add an exception that prevents scanning of the folders that contain the Microsoft SQL Server database files. These exceptions improve performance and avoid corruption or files being locked when the Microsoft SQL Server must use them. For more information, see the knowledge base article: How to exclude MS SQL files and folders using Centralized Exceptions. You can also exclude files by extension for Auto-Protect scans on Windows computers.
Run a quick report and scheduled report after the scheduled scan	Run the quick reports and scheduled reports to see whether the client computers have the correct level of security.
Check to ensure that scheduled scans have been successful and clients operate as expected	Review monitors, logs, and the status of client computers to make sure that you have the correct level of protection for each group.

Table 1-5 Tasks to perform two weeks after you install *(continued)*

Action	Description
Configure the content revisions available to clients to reduce bandwidth	Set the number of content revisions that are stored on the management server to reduce bandwidth usage for clients. The more content revisions that the client stores, the clients are likely to download a smaller incremental package. However, you should balance bandwidth usage with the amount of hard disk space. ■ Typically, three content updates are delivered per day. You configure the number of updates that are retained on the server. You generally want to store only the most recent content updates. A client that has not connected during the time it takes the server to accumulate the set number of updates, downloads an entire content package. An entire package is typically larger than 100 MB. An incremental update is between 1 MB and 2 MB. You configure the number of stored updates to minimize how often a client must download a complete update package. ■ As a general rule, 1content revision uses about 1.4 GB of disk space on the Symantec Endpoint Protection Manager. When LiveUpdate for the management server is set to the default of every four hours, 10 content revisions cover at least three days. For more information about calculating storage and bandwidth needs, see the Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper.
Configure notifications for a single risk outbreak and when a new risk is detected	Create a notification for a **Single risk event** and modify the notification for **Risk Outbreak**. For these notifications, Symantec recommends that you do the following actions: 1 Change the **Risk severity** to **Category 1 (Very Low and above)** to avoid receiving emails about tracking cookies. 2 Keep the **Damper** setting at **Auto**. Notifications are critical to maintaining a secure environment and can also save you time.
Increase the time that the console leaves you logged on	The console logs you out after one hour. You can increase this period of time.

For information on how to perform these tasks, see the *Symantec Endpoint Protection and Symantec Network Access Control Installation and Administration Guide*.

See the knowledge base article, Top "Best Practices" Articles for Symantec Endpoint Protection.

System requirements for Symantec Endpoint Protection

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 1-6 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 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 ■ Google Chrome

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

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

- 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 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*.

For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

Installing Symantec Endpoint Protection Manager

You perform several tasks to install the management server and the console. In the installation wizard, a green check mark appears next to each completed task.

Note: The Symantec Endpoint Protection Manager requires access to the system registry for installation and normal operation. To prepare a server that runs Windows Server 2003 to install Symantec Endpoint Protection Manager using a remote desktop connection, you must first allow remote control on the server. You must also use a remote console session, or shadow the console session.

For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

See "Getting up and running on Symantec Endpoint Protection for the first time" on page 12.

To install Symantec Endpoint Protection Manager

1. Insert and display the product disc.

   The installation should start automatically. If it does not start, double-click **Setup.exe**.

   If you downloaded the product, extract the entire product disc image to a physical disc, such as a hard disk. Run **Setup.exe** from the physical disc.

2. In the **Symantec Endpoint Protection Installation Program** dialog box, click **Install Symantec Endpoint Protection**, and then click **Install Symantec Endpoint Protection Manager**.

3. Review the sequence of installation events, and then click **Next** to begin.

4. In the **License Agreement** panel, click **I accept the terms in the license agreement**, and then click **Next**.

5. In the **Destination Folder** panel, accept the default destination folder or specify another destination folder, and then click **Next**.

6. Click **Install**.

   The installation process begins for the Symantec Endpoint Protection Manager and console. When the installation is complete, click **Next**.

7. After the initial installation completes, you configure the server and database. Click **Next**.

   The **Management Server Configuration Wizard** starts.

   See "Configuring the management server during installation" on page 22.

8. You configure the management server according to your requirements. Follow the on-screen instructions. After the server and the database configuration, click **Next** to create the database.

9. Click **Finish** to complete the configuration.

   The Symantec Endpoint Protection Manager console log on screen appears if you leave the option checked. Once you log in, you can begin client deployment. You can also optionally run the Migration Wizard at this time, if desired.

   See "Deploying clients using a Web link and email" on page 25.

Configuring the management server during installation

The Management Server Configuration Wizard automatically starts after the Symantec Endpoint Protection Manager installation.

See "Installing Symantec Endpoint Protection Manager" on page 20.

You can also start the Management Server Configuration Wizard at any time after installation from **Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools**.

To configure the server, you specify the following information:

- The configuration type: default or custom. The wizard provides information about each type.
- Whether you want to use a recovery file.

  Note: If this is your first installation of Symantec Endpoint Protection Manager, there is no recovery file.

- The password for the default administrator account.
- The email address that receives important notifications and reports.
- The email server name and port number.
- You can optionally add partner information if you have a Symantec Sales Partner who manages your Symantec licenses.

Each configuration type has a separate configuration process. Follow the instructions that are provided in the Management Server Configuration Wizard to complete the configuration.

Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license

You can use the License Activation Wizard workflow to perform the following tasks:

- Activating a new paid license.
- Converting a trial license to a paid license.
- Renewing a license.

- Activating a license after you upgrade from a previous version, such as Symantec Endpoint Protection 11.x.
- Activating an additional paid license in response to an over-deployment status.

You can import and activate a license file that you received from the following sources:

- Symantec Licensing Portal
- Symantec partner or preferred reseller
- Symantec sales team
- Symantec Business Store

You can start the License Activation Wizard in the following ways:

- The Symantec Endpoint Protection Welcome screen that appears after you install the product.
- From the **Common Tasks** menu on the **Home** page.
- The **Admin** page of the Symantec Endpoint Protection Manager console.

If you activate or import your license from the Welcome screen or the **Common Tasks** menu, you can skip the first three of the following steps.

To activate or import your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license

1. On the Symantec Endpoint Protection Manager console, click **Admin**.
2. On the **Admin** page, click **Licenses**.
3. Under **Tasks**, click **Activate license**.
4. In the **License Activation Wizard**, select **Activate a new license**, and then click **Next**. If you do not see this panel, continue to the next step.

5 On the **License Activation** panel, select the option that matches your situation, and then click **Next**.

The following table describes each option:

Option	Description
I have a serial number	You may receive a license serial number when you or your Symantec Partner purchased the license. If you have a license serial number, select this option. If you are an eFlex (Symantec Enterprise Options) customer and have an eFlex-generated serial number, select **I have a Symantec License File**.
I have a Symantec License File (.slf)	In most cases, a Symantec license file (.slf file) is sent to you in an email from Symantec shortly after you complete the purchase process. The file arrives attached to the notification email as a .zip file. If you have received a .slf file, select this option. **Note:** You must extract the .slf file from the .zip file before you can use it to activate your product license. **Warning:** The .slf file contains the information that is unique to your license. To avoid corrupting the license file, do not alter its contents. You may copy the file for your records.

You can find information about eFlex at the following URL:

Enterprise Options

6 Do one of the following tasks based on the selection that you made in the previous step:

- If you selected **I have a serial number**, enter the serial number, and then click **Submit**. Review the information about the license you added, and then click **Next**.
- If you selected **I have a Symantec License File (.slf)**, click **Add File**. Browse to and select the .slf file you extracted from the .zip file that was attached to your Symantec notification email. Click **Open**, and then click **Next**.

7 Enter information about your technical contacts and primary contacts, and about your company. Click to acknowledge the disclosure statement, and then click **Submit**.

If you provided this information when you purchased your license, this panel does not display.

8 Click **Finish**.

You can also view a video walkthrough of Symantec Endpoint Protection.

To view the video walkthrough

1 Go to http://go.symantec.com/education_septc.

2 On the linked page, click **Symantec Endpoint Protection 12.1**.

3 On the expanded list, click **Symantec Endpoint Protection 12.1: How to Activate the License**.

See "Getting up and running on Symantec Endpoint Protection for the first time" on page 12.

Deploying clients using a Web link and email

The Web link and email method creates a URL for each client installation package. You send the link to users in an email or make it available from a network location.

Web link and email performs the following actions:

- Selects and configures the client installation packages.
  Client installation packages are created for 32-bit and 64-bit Windows computers. The installation packages are stored on the computer that runs Symantec Endpoint Protection Manager.
- Notifies the computer users about the client installation packages.
  An email message is sent to the selected computer users. The email message contains instructions to download and install the client installation packages. Users follow the instructions to install the client software.

The Mac client install package is automatically exported as a `.zip` archive file. To expand the package and extract the folder containing the Apple installer file (`.pkg`) and the `Additional Resources` folder, you must use either the Mac `Archive Utility` or the `ditto` command. You cannot use the Mac `unzip` command, a third-party application, or any Windows application to expand this file. You must keep the `.pkg` file and the `Additional Resources` folder together to complete the installation successfully.

Before you deploy the client installation package with email, make sure that you correctly configure the connection from the management server to the mail server.

You start the client deployment from the console.

To deploy clients by using a Web link and email

1. In the console, on the **Home** page, in the **Common Tasks** menu, select **Install protection client to computers**.
2. In the **Client Deployment Wizard**, click **New Package Deployment** to create a new installation package, and then click **Next**.

   Existing Package Deployment lets you deploy the packages that have been exported previously, but you can only use Remote Push with this option.

   Communication Update Package Deployment lets you update client communication settings on the computers that already have the client installed. Use this option to convert an unmanaged client to a managed client. You can only use Remote Push or Save Package with this option.
3. For a new package, make selections from **Install Packages**, **Group**, **Install Feature Sets**, **Install Settings**, **Content Options**, and **Preferred Mode**. Click **Next**.

   Note: To uninstall third-party security software on the client, you must configure custom Client Install Settings before launching the Client Deployment Wizard. To see which third-party software the client package removes, see the following knowledge base article: About the third-party security software removal feature in Symantec Endpoint Protection 12.1.
4. Click **Web Link and Email**, and then click **Next**.

5 In the **Email Recipients and Message** panel, specify the email recipients and the subject.

To specify multiple email recipients, type a comma after each email address. A management console System Administrator automatically receives a copy of the message.

You can accept the default email subject and body, or edit the text. You can also copy the URL and post it to a convenient online location, like an intranet page.

To create the package and deliver the link by email, click **Next**, and then click **Finish**.

6 Confirm that the computer users received the email message and installed the client software.

Client computers may not appear within the management console until after they are restarted. Depending on the client restart settings of the deployed client, you or the computer users may need to restart the client computers.

Where to get more information about Symantec Endpoint Protection

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:

- Endpoint Protection

The product includes the following documentation:

- *Symantec Endpoint Protection Getting Started Guide*
- *Symantec Endpoint Protection and Symantec Network Access Control Installation and Administration Guide*
- *Symantec Endpoint Protection and Symantec Network Access Control 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 1-8 displays the Web sites where you can get additional information to help you use the product.

Table 1-8 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	http://www.symantec.com/business/support/overview.jsp? pid=54619
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