Symantec™ Endpoint Protection 12.1.5 Getting Started Guide

Symantec Endpoint Protection Getting Started Guide

Product version: 12.1.5

Documentation version: 1

This document was last updated on: September 17, 2014

Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, LiveUpdate, and TruScan are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Getting Started with Symantec Endpoint Protection

This document includes the following topics:

What is Symantec Endpoint Protection?

Symantec Endpoint Protection is a client-server solution that protects laptops, desktops, and servers in your network against malware, risks, and vulnerabilities. Symantec Endpoint Protection combines virus protection with advanced threat protection to proactively secure your client computers against known and unknown threats, such as viruses, worms, Trojan horses, and adware. Symantec Endpoint Protection 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 both physical systems and virtual systems against attacks. Symantec Endpoint Protection provides management solutions that are efficient and easy to deploy and use.

Symantec Endpoint Protection protects your network by accomplishing the following key tasks:

- Protects your endpoints from malware and maximizes system uptime.
  See "How Symantec Endpoint Protection uses layers to protect computers" on page 14.
- Enforces protection policies and compliance on the endpoint.
  See "How does Symantec Endpoint Protection enforce compliance?" on page 17.
- Responds to threats and incidents effectively by quickly quarantining and removing malware from endpoints.
- Monitors and tracks risk exposure across platforms, devices, remote locations, and in physical, virtual or hybrid environments.

See "Components of Symantec Endpoint Protection" on page 17.

What's new in Symantec Endpoint Protection 12.1.5

Note: Symantec Endpoint Protection 12.1.5 is the last release update to support Symantec Protection Center 2.0.

In addition, LiveUpdate Administration Utility 1.x reaches end of life on January 5, 2015. If you use this utility in your environment, you should migrate to LiveUpdate Administrator 2.3.x. To get the latest version of LiveUpdate Administrator, see Downloading LiveUpdate Administrator.

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

Table 1-1 New features in Symantec Endpoint Protection 12.1.5

Feature	Description
OpenSSL 1.0.1h for Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager now uses OpenSSL 1.0.1h. The update to OpenSSL addresses several security vulnerabilities, including the one known as Heartbleed, which the OpenSSL Security Advisory for CVE-2014-0160 describes. Earlier versions of OpenSSL can reveal sensitive information from the computer's memory to a remote attacker. You can read the full text of the OpenSSL Security Advisory at the following link: OpenSSL Security Advisory for CVE-2014-0160
System requirements	The Symantec Endpoint Protection client for Linux replaces the Symantec AntiVirus client for Linux and supports a greater range of distributions and kernels. Added distributions include Red Hat Enterprise Linux Server (RHEL) 6.5 and CentOS 6.5. Symantec Endpoint Protection 12.1.5 adds the following operating system support: ■ Windows 8.1 Update 2 ■ Windows Server 2012 Update 2 ■ Mac OS X 10.10 You can now access Symantec Endpoint Protection Manager from the following browsers: ■ Microsoft Internet Explorer 10.2, 11 ■ Mozilla Firefox 5.x through 31.0 ■ Google Chrome through 37.0.2062.94 For the complete list of system requirements: See “System requirements for Symantec Endpoint Protection” on page 8.

Table 1-1 New features in Symantec Endpoint Protection 12.1.5 *(continued)*

Feature	Description
Windows client protection features	The Windows client provides the following new protection enhancements: Virus and Spyware Protection: ■ Power Eraser can now be run from the Symantec Endpoint Protection Manager console. Power Eraser provides aggressive scanning and analysis to help resolve issues with heavily infected Windows computers. You should only run Power Eraser in emergency situations, such as when a repair fails or a computer is unstable. Note that when you run Power Eraser from the management console, Power Eraser does not scan and analyze user-specific locations. Use Power Eraser in the SymHelp tool directly on the client computer to examine user-specific locations. ■ Download Insight and SONAR can now scan Office 2013 applications. ■ The client no longer scans and deletes backed up files on a server where the Symantec Endpoint Protection client and either Symantec Backup Exec or Symantec NetBackup is installed. Network Threat Protection: ■ For firewall rules, you can now define a host group with an IPv6 IP address. Intrusion Prevention policies do not support host names with IPv6 addresses. The default firewall policy includes a default **Allow ICMPv6** firewall rule that contains ICMPv6 types of 1-4,128-132,141-143,148,149,151-153. You can also add a rule with ICMPv6 as a protocol in the network service list. ■ You can now use SHA-256 checksums as well as MD5 checksums for file fingerprints in the firewall rules and the application learning feature. ■ IPS audit signatures monitor the network traffic of certain applications on Windows computers. For example, you can use these signatures to detect Yahoo IM logons. You can enable logging, review the Network Threat Protection traffic logs, and then decide whether or not to take action on the traffic.
Linux management	The Symantec Endpoint Protection for Linux client replaces the Symantec AntiVirus for Linux client. You can now provide Virus and Spyware Protection on the clients that run Linux. Symantec Endpoint Protection Manager provides client policy management, reporting, monitoring, logging, and licensing in a single client package for Linux.
Policy enforcement	The Host Integrity policy is now included with Symantec Endpoint Protection. The Host Integrity policy evaluates the client computers and ensures that they meet the security policies you have downloaded to those client computers.

Table 1-1 New features in Symantec Endpoint Protection 12.1.5 *(continued)*

Feature	Description
Management server updates	■ You can now remotely deploy the Mac client installation package in addition to deploying it with a third-party installation tool. See "Installing clients with Remote Push" on page 36. ■ Symantec Protection Center 1 is removed for Symantec Endpoint Protection 12.1.5. You can still integrate Symantec Endpoint Protection Manager with Symantec Protection Center 2, but the feature is no longer tested or available for download. ■ You can configure the installation package to remove from the client computer over 300 third-party software products from more than 60 vendors. For more information, see: Third-party security software removal support in Symantec Endpoint Protection ■ Client password settings dialog box The client password protection settings now appear in a more accessible location in **Clients** > **Policies** > **Password Settings**. This dialog also provides a new option to enable password protection globally for all clients. You can also access the **Password Settings** dialog box when you log on to Symantec Endpoint Protection Manager. ■ You can no longer set the console timeout to **Never**. For security reasons, the maximum timeout period is one hour. ■ After an administrator's failed logon attempts trigger an account lockout, the lockout interval now doubles with each subsequent lockout. Symantec Endpoint Protection Manager reverts to the original lockout interval after a successful logon, or after 24 hours since the first lockout.
Management server integration with network security technology	Web services on the management server now support integration with Symantec Managed Security Services. Together, Symantec Managed Security Services and Symantec Endpoint Protection Manager provide advanced threat monitoring and targeted remediation options. The following new web services are also available for use by third-party remote monitoring and management solutions: ■ You can run the new Power Eraser commands. ■ You can place clients into Quarantine. ■ You can run an Evidence of Compromise command on the client. Documentation and other tools for remote monitoring and management support appear in the web services SDK. The SDK is located in the Tools installation file in the following folder: `/Integration/SEPM_WebService_SDK`
Management server integration with advanced reporting	Symantec Endpoint Protection 12.1.5 comes with a new version of IT Analytics. This new version removes the need for the Symantec Management Platform, supports most common browsers, requires no plug-ins, and also supports mobile devices. IT Analytics delivers advanced reporting and query capability for customers who want more sophisticated reporting than Symantec Endpoint Protection Manager can provide alone. The IT Analytics installer is located in the Tools installation file in the following folder: `/ITAnalytics`

Table 1-1 New features in Symantec Endpoint Protection 12.1.5 *(continued)*

Feature	Description
Management server and client performance	The management server and the client include the following performance improvements: ■ Bandwidth control for client communication The management server now includes an Apache module that you can configure to control network bandwidth. The module reduces the network load between Symantec Endpoint Protection Manager and the client computers, especially when the clients download content definitions or client installation packages. ■ To reduce hard disk space, Symantec Endpoint Protection Manager now stores only the most recent full set of virus definitions, plus the deltas for previous versions. Storing the deltas reduces delivery time and network bandwidth, and improves disk storage requirements on the management server by 65% to 80%. ■ The client startup time has improved by more than 10%. ■ The client service needs fewer processes to run. ■ Enhancements to the scan throttling logic for the Windows client improve scan performance. These enhancements also minimize the effect on computers with solid-state drives (SSDs) or that run in a virtualized or Terminal Services environment. ■ If Symantec Endpoint Protection and Critical System Protection are both installed on the same client computer, these applications now share Symantec components.
Documentation	Symantec Endpoint Protection provides the following documentation changes: ■ The main PDF files are now on the Technical Support site. You can now look for and download the most current PDF files from a single location: ■ Product guides for all versions of Symantec Endpoint Protection and Symantec Endpoint Protection Business Edition (English) ■ Symantec Endpoint Protection (all other languages) The documents for specific tools remain in the same folder as the associated tool. ■ The *Symantec Endpoint Protection Installation and Administration Guide* no longer includes Network Access Control topics. A new *Symantec Network Access Control Installation and Administration Guide* includes the Network Access Control topics.

System requirements for Symantec Endpoint Protection

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

For the most current system requirements, see:

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

- System requirements for Symantec Endpoint Protection Manager
  See "System requirements for Symantec Endpoint Protection Manager" on page 9.
- System requirements for the Symantec Endpoint Protection client for Windows
  See "System requirements for the Symantec Endpoint Protection client for Windows" on page 11.
- System requirements for the Symantec Endpoint Protection client for Mac
  See "System requirements for the Symantec Endpoint Protection client for Mac" on page 12.
- System requirements for the Symantec Endpoint Protection client for Linux
  See "System requirements for the Symantec Endpoint Protection client for Linux" on page 13.

See "Getting up and running on Symantec Endpoint Protection for the first time" on page 20.

System requirements for Symantec Endpoint Protection Manager

Table 1-2 displays the minimum requirements for Symantec Endpoint Protection Manager.

Table 1-2 Symantec Endpoint Protection Manager system requirements

Component	Requirements
Processor	■ 32-bit processor: Intel Pentium 4 or equivalent (minimum dual core or hyper-threading recommended) ■ 64-bit processor: Intel Pentium 4 with x86-64 support or equivalent (minimum dual core or hyper-threading recommended) **Note:** Intel Itanium IA-64 processors are not supported.
Physical RAM	2 GB RAM available minimum; 4 GB or more available recommended. **Note:** Your Symantec Endpoint Protection Manager server may require additional RAM depending on the RAM requirements of other applications that are already installed.
Hard drive	16 GB available minimum (100 GB recommended) for the management server. 40 GB available minimum (200 GB recommended) for the management server and a locally installed database.
Display	1024 x 768

Table 1-2 Symantec Endpoint Protection Manager system requirements *(continued)*

Component	Requirements
Operating system	■ Windows XP (32-bit, SP2 or later; 64-bit, all SPs; all editions except Home) ■ Windows 7 (32-bit, 64-bit; RTM and SP1; all editions except Home) ■ Windows 8 (32-bit, 64-bit) ■ Windows 8.1 (32-bit, 64-bit) ■ Windows 8.1 Update 1 (32-bit, 64-bit) ■ Windows 8.1 Update 2 (32-bit, 64-bit) ■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit; R2, RTM, SP1 and SP2) ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows Server 2012 R2 Update 1 ■ Windows Server 2012 R2 Update 2 ■ 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 8, 9, 10, 10.2, 11 ■ Mozilla Firefox 3.6 through 31.0 ■ Google Chrome, through 37.0.2062.94

Note: This Symantec Endpoint Protection Manager version manages clients earlier than 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, through SP3
- SQL Server 2008 R2, through SP2
- SQL Server 2012, through SP1
- SQL Server 2014

System requirements for the Symantec Endpoint Protection client for Windows

Table 1-3 displays the minimum requirements for the Windows client.

Table 1-3 Symantec Endpoint Protection client for Windows 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:** Itanium processors are not supported.
Physical RAM	512 MB of RAM (1 GB recommended), or higher if required by the operating system
Hard drive	1.8 GB 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.
Display	800 x 600

Table 1-3 Symantec Endpoint Protection client for Windows 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 7 Embedded Standard ■ Windows 8 (32-bit, 64-bit) ■ Windows 8 Embedded (32-bit) ■ Windows 8.1 (32-bit, 64-bit), including Windows To Go ■ Windows 8.1 Update 1 (32-bit, 64-bit) ■ Windows 8.1 Update 2 (32-bit, 64-bit) ■ Windows 8.1 Embedded (32-bit) ■ Windows Server 2003 (32-bit, 64-bit; R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit; R2, SP1, and SP2) ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows Server 2012 R2 Update 1 ■ Windows Server 2012 R2 Update 2 ■ 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)

System requirements for the Symantec Endpoint Protection client for Mac

Table 1-4 displays the minimum requirements for the Mac client.

Table 1-4 Symantec Endpoint Protection client for Mac system requirements

Component	Requirements
Processor	Intel Core 2 Duo, Intel Quad-Core Xeon
Physical RAM	2 GB of RAM
Hard drive	1 GB of available hard disk space for the installation
Display	800 x 600

Table 1-4 Symantec Endpoint Protection client for Mac system requirements *(continued)*

Component	Requirements
Operating system	Mac OS X 10.8, 10.9, 10.10

System requirements for the Symantec Endpoint Protection client for Linux

Table 1-5 displays the minimum requirements for the Linux client.

Table 1-5 Symantec Endpoint Protection client for Linux system requirements

Component	Requirements
Hardware	■ Intel Pentium 4 (2 GHz) or higher processor ■ 1 GB of RAM ■ 5 GB of available hard disk space
Operating systems	■ CentOS 6U4, 6U5; 32-bit and 64-bit ■ Debian 6.0.5 Squeeze; 32-bit and 64-bit ■ Fedora 16, 17; 32-bit and 64-bit ■ Novell Open Enterprise Server (OES) 2 SP2 and 2 SP3 running SUSE Linux Enterprise Server (SLES) 10 SP3; 32-bit and 64-bit ■ Novell Open Enterprise Server (OES) 11 and 11 SP1 running SUSE Linux Enterprise Server (SLES) 11 SP1 and SP2; 64-bit ■ Oracle Linux 5U8, 5U9, 6U2, 6U4; 64-bit ■ Red Hat Enterprise Linux Server (RHEL) 5U7 - 5U10, 6U2 - 6U5; 32-bit and 64-bit ■ SUSE Linux Enterprise Server (SLES) 10 SP3, 10 SP4, 11 SP1 - 11 SP3; 32-bit and 64-bit ■ SUSE Linux Enterprise Desktop (SLED) 10 SP3, 10 SP4, 11 SP1 - 11 SP3; 32-bit and 64-bit ■ Ubuntu Server 11.10, 12.04, 12.04.2, 13.04; 64-bit ■ Ubuntu Desktop 11.10, 12.04, 12.04.2, 13.04; 64-bit For a list of supported kernels, see: http://entced.symantec.com/sep/12.1.5/doc_sep_linux_sys_req
Graphical desktop environments	You can use the following graphical desktop environments to view the Symantec Endpoint Protection client's graphical user interface: ■ KDE ■ Gnome

Table 1-5 Symantec Endpoint Protection client for Linux system requirements *(continued)*

Component	Requirements
Other environmental requirements	■ Oracle Java 1.5 or later; Java 7 or later recommended. This installation requires superuser privileges. ■ Unlimited Strength Java Cryptography Extension (JCE) You must install the Unlimited Strength Java Cryptography Extension policy files to match your version of Java. This installation requires superuser privileges. You can download the installation files under **Additional Resources** from the following Oracle website: http://www.oracle.com/technetwork/java/javase/downloads/index.html ■ i686-based dependent packages on 64-bit computers Many of the executable files in the Symantec Endpoint Protection package are 32-bit programs. For 64-bit computers that run Fedora Linux, you must install the i686-based dependent packages before you install the Symantec Endpoint Protection package. If you have not already installed the i686-based dependent packages on the Fedora Linux computer, you can install them with the following command. This installation requires superuser privileges, which the following command demonstrates with `sudo`: `sudo yum install glibc.i686 libgcc.i686 libX11.i686`

How Symantec Endpoint Protection uses layers to protect computers

Symantec's core protection against known and unknown threats uses a layered approach to defense. The layered approach protects the network before, during, and after an attack. Symantec Endpoint Protection reduces your risk of exposure by providing tools to increase your security posture ahead of any attack.

Table 1-6 describes the types of protection that Symantec Endpoint Protection Manager uses to protect your network.

Table 1-6 The layers of protection that are integrated into Symantec Endpoint Protection

Layer	Type of protection	Description	Symantec Endpoint Protection technology name
1	Network-based protection	The firewall and the intrusion prevention system block over 60% of malware as it travels over the network and before it arrives at the computer. This primary defense protects against drive-by downloads, social engineering, fake antivirus programs, individual system vulnerabilities, rootkits, botnets, and more. Stopping malware before it reaches your computer is definitely preferred to identifying a vulnerability that has already been exploited.	Network Threat Protection: ■ Firewall ■ Protocol-aware IPS Virus and Spyware Protection: ■ Browser protection
2	File-based protection	This traditional signature-based antivirus protection looks for and eradicates the malware that has already taken up residence on a system. Virus and Spyware Protection blocks and removes the malware that arrives on the computer by using scans. Unfortunately, many companies leave themselves exposed through the belief that antivirus alone keeps their systems protected.	Virus and Spyware Protection: ■ Antivirus engine ■ Auto-Protect ■ Bloodhound
3	Reputation-based protection	Insight establishes information about entities, such as websites, files, and IP addresses to be used in effective security. Download Insight determines the safety of files and websites by using the wisdom of the community. Sophisticated threats require leveraging the collective wisdom of over 200 million systems to identify new and mutating malware. Symantec's Insight gives companies access to the largest global intelligence network available to allow them to filter every file on the internet based on reputation.	Virus and Spyware Protection: ■ Domain reputation score ■ File reputation (Insight)

Table 1-6 The layers of protection that are integrated into Symantec Endpoint Protection *(continued)*

Layer	Type of protection	Description	Symantec Endpoint Protection technology name
4	Behavioral-based protection	SONAR looks at processes as they execute and use malicious behaviors to indicate the presence of malware. SONAR watches programs as they run, and blocks suspicious behaviors. SONAR catches targeted and unknown threats by aggressively monitoring file processes as they execute and identify malicious behavior. SONAR uses artificial intelligence, behavior signatures, and policy lockdown to monitor nearly 1,400 file behaviors as they execute in real time. When SONAR is combined with Insight, this technology is able to aggressively stop zero-day threats without increasing false-positives.	■ Proactive Threat Protection (Virus and Spyware Protection policy): SONAR
5	Repair and remediation tools	When malware does get through, Power Eraser scrubs hard-to-remove infections and gets your system back online as quickly as possible. Power Eraser uses aggressive remediation on hard-to-remove infections.	Power Eraser: ■ Boot to clean operating system ■ Power Eraser uses aggressive heuristics ■ Threat-specific tools

Symantec Endpoint Protection extends and enhances security with the following additional technologies:

- System Lockdown
  System Lockdown lets you limit the applications that can run. System Lockdown operates in either a whitelisting or a blacklisting mode. In either mode, System Lockdown uses checksum and file location parameters to verify whether an application is approved or unapproved. System Lockdown is useful for kiosks where you want to run a single application only.
- Application control
  Application control monitors and controls an application's behavior.
  Application control protects against unauthorized access and attack by controlling what applications can run. Application control blocks or terminates processes, limits file and folder access, protects the Windows registry, and controls module and DLL loading. Application control includes predefined templates that block application behaviors known to be malicious.

- Device control
  Device control restricts and enables the access to the hardware that can be used on the client computer. You can block and control the devices that are connected to your systems, such as USB devices, FireWire, serial, and parallel ports. Device control can prevent all access to a port or allow access only from certain devices with a specific vendor ID.

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

How does Symantec Endpoint Protection enforce compliance?

Symantec Endpoint Protection also ensures that the client computers meet compliance requirements. You may need to enforce the company's security policy, such as blocking computers from opening certain applications or websites. Or, you may need to prevent security breaches and enforce security and privacy-related regulations. For example, Symantec solutions help healthcare organizations to enforce healthcare data provisions against medical identity theft.

Symantec Endpoint Protection uses the following tools to enforce compliance requirements:

- Host Integrity
  The Host Integrity policy ensures that the endpoints are protected and compliant. For example, you can make sure that every computer is running a firewall or a particular operating system security patch.
- Reporting and analytics
  Symantec Endpoint Protection provides multi-dimensional analysis, robust graphical reporting, and an easy-to-use Dashboard. You can use reports and logs to check that the computers in your network are connected, protected, and compliant with company policy.

See "How Symantec Endpoint Protection uses layers to protect computers" on page 14.

Components of Symantec Endpoint Protection

Table 1-7 describes the main components of Symantec Endpoint Protection.

Table 1-7 Main 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 subcomponents: ■ 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. ■ The embedded database stores security policies and events and is installed with Symantec Endpoint Protection Manager. You can also install a SQL Server database to use instead of the embedded database. See "Installing Symantec Endpoint Protection Manager" on page 25.
Symantec Endpoint Protection client	The Symantec Endpoint Protection client runs on the following platforms: ■ The Windows client protects computers by using 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 computers by using virus and spyware scans and an intrusion prevention system. ■ The Symantec Endpoint Protection Linux client protects computers by using virus and spyware scans. See "What is Symantec Endpoint Protection?" on page 4.

See "Optional components for Symantec Endpoint Protection" on page 18.

See "How Symantec Endpoint Protection uses layers to protect computers" on page 14.

Optional components for Symantec Endpoint Protection

Table 1-8 lists the additional components that you can download and use with Symantec Endpoint Protection.

Table 1-8 Optional components and their function

Component	Description
LiveUpdate Administrator	LiveUpdate Administrator downloads definitions, signatures, and product updates from an internal LiveUpdate server and distributes the updates to client computers. You can use an internal LiveUpdate server in very large networks to reduce the load on the Symantec Endpoint Protection Manager. You should also use the internal LiveUpdate server if your organization runs multiple Symantec products that also use LiveUpdate to update client computers. The LiveUpdate Administrator is located in the LiveUpdate folder in the Tools installation file.
Group Update Provider (GUP)	The Group Update Provider helps distribute content within the organization, particularly useful for groups at remote locations with minimal bandwidth. Organizations that have a lot of clients may want to use Group Update Providers (GUPs) for Windows clients. GUPs reduce the load on the management server and are easier to set up than an internal LiveUpdate server.
Central Quarantine	The Central Quarantine receives suspicious files and unrepaired infected items from the Symantec Endpoint Protection clients. The Central Quarantine forwards a sample to Symantec Security Response, which analyzes the sample. If a threat is new, Symantec Security Response produces security updates. The Central Quarantine is located in the Tools\CentralQ folder. For more information, see the *Symantec Central Quarantine Implementation Guide*.
Shared Insight Cache and Security Virtual Appliance	These components enhance the scanning on virtual environments. The Symantec Endpoint Protection Security Virtual Appliance is a Linux-based virtual appliance that you install on a VMware ESX/ESXi server. The Security Virtual Appliance integrates with VMware's vShield Endpoint. The Shared Insight Cache runs in the appliance and lets Windows-based Guest Virtual Machines (GVMs) with the Symantec Endpoint Protection client installed share scan results. The virtualization tools are located in the Tools\Virtualization folder.
IT Analytics server	The IT Analytics tool expands upon the built-in reports in Symantec Endpoint Protection Manager by enabling you to create custom reports and custom queries. The tool also offloads the reporting burden from the management server to another server. IT Analytics keeps information for a longer period of time, enforces compliance, reduces costs, and provides summaries. The IT Analytics tool and documentation is located in the Tools\ITAnalytics folder.

See "Components of Symantec Endpoint Protection" on page 17.

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 1-9 lists the tasks that you should perform to install and protect the computers in your network immediately.

Table 1-9 Tasks to install and configure Symantec Endpoint Protection

Action	Description
Plan your installation structure	Before you install the product, consider the size and geographical distribution of your network to determine the installation architecture. To ensure good network and database performance, you need to evaluate several factors. These factors include how many computers need protection, whether any of those computers connect over a wide-area network, or how often to schedule content updates. ■ If your network is small, is located in one geographic location, and has fewer than 500 clients, you need to install only one Symantec Endpoint Protection Manager. ■ If the network is very large, you can install additional sites with additional databases and configure them to share data with replication. To provide additional redundancy, you can install additional sites for failover or load balancing support. Failover and load balancing can only be used with Microsoft SQL Server databases. ■ If your network is geographically dispersed, you may need to install additional management servers for load balancing and bandwidth distribution purposes. To help you plan medium to large-scale installations, see: Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper.

Table 1-9 Tasks to install and configure Symantec Endpoint Protection *(continued)*

Action	Description
Prepare for and then install Symantec Endpoint Protection Manager	**1** Make sure the computer on which you install the management server meets the minimum system requirements. See: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control **2** To install Symantec Endpoint Protection Manager, you must be logged on with an account that grants local administrator access. **3** Decide on whether to install the embedded database or use a Microsoft SQL Server database. If you use a Microsoft SQL Server database, the installation requires additional steps. These include, but are not limited to, configuring or creating a database instance that is configured to use mixed mode or Windows authentication mode. You also need to provide database server administration credentials to create the database and the database user. These are specifically for use with the management server. **4** You install Symantec Endpoint Protection Manager first. After you install, you immediately configure the installation with the Management Server Configuration Wizard. Decide on the following items when you configure the management server: ■ A password for your login to the management console ■ An email address where you can receive important notifications and reports ■ An encryption password, which may be needed depending on the options that you select during installation See “Installing Symantec Endpoint Protection Manager” on page 25. See “Configuring Symantec Endpoint Protection Manager during installation” on page 27.

Table 1-9 Tasks to install and configure Symantec Endpoint Protection *(continued)*

Action	Description
Add groups, policies, and locations	1 You use groups to organize the client computers, and apply a different level of security to each group. You can use the default groups, import groups if your network uses Active Directory or an LDAP server, or add new groups. If you add new groups, you can use the following group structure as a basis: ■ Desktops ■ Laptops ■ Servers 2 You use locations to apply different policies and settings to computers based on specific criteria. For example, you can apply different security policies to the computers based on whether they are inside or outside the company network. In general, the computers that connect to your network from outside of your firewall need 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. See Best Practices for Symantec Endpoint Protection Location Awareness. 3 Disable inheritance for the groups or locations for which you want to use different policies or settings. By default, groups inherit their policies and settings from the default parent group, **My Company**. If you want to assign a different policy to child groups, or want to add a location, you must first disable inheritance. Then you can change the policies for the child groups, or you can add a location. 4 For each type of policy, you can accept the default policies, or create and modify new policies to apply to each new group or location. You must add requirements to the default Host Integrity policy for the Host Integrity check to have an effect on the client computer..
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. For fewer than 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. Symantec recommends that you leave **Let clients upload critical events immediately** checked. ■ Increase the download randomization to between one and three times the heartbeat interval.

Table 1-9 Tasks to install and configure Symantec Endpoint Protection *(continued)*

Action	Description
Activate the product license	Purchase and activate a license within 60 days of product installation. See "Activating or importing your Symantec Endpoint Protection 12.1.x product license" on page 27.

Decide on a client deployment method	Determine which client deployment method would work best to install the client software on your computers in your environment.
	
	■ For Linux clients, you can use either Save Package or Web Link and Email, but not Remote Push.
	■ For Windows and Mac clients, if you use Remote Push, you may need to do the following tasks:
	  ■ Make sure that administrator access to remote client computers is available. Modify any existing firewall settings (including ports and protocols) to allow remote deployment between Symantec Endpoint Protection Manager and the client computers.
	  ■ You must be logged on with an account that grants local administrator access. If the client computers are part of an Active Directory domain, you must be logged on to the computer that hosts Symantec Endpoint Protection Manager with an account that grants local administrator access to the client computers. You should have administrator credentials available for each client computer that is not part of an Active Directory domain.

Table 1-9 Tasks to install and configure Symantec Endpoint Protection *(continued)*

Action	Description
Prepare and deploy the client software for installation	1 Make sure that the computers on which you install the client software meet the minimum system requirements. See: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control 2 Manually uninstall any third-party security software programs from Windows computers that the Symantec Endpoint Protection client installer cannot uninstall. For a list of products that this feature removes, see: Third-party security software removal support in Symantec Endpoint Protection You must uninstall any existing security software from Linux computers or from Mac computers. Some programs may also have special uninstallation routines. See the documentation for the third-party software. 3 For Windows clients, do the following tasks: ■ Create a custom client install feature set to determine which components you install on the client computers. You can also use one of the default client install feature sets. Make sure that you keep computer mode and 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**. ■ Update custom client install settings to determine installation options on the client computer. These options include the target installation folder, the uninstallation of third-party security software, and the restart behavior after installation completes. You can also use the default client install settings. 4 With the Client Deployment Wizard, create a client installation package with selections from the available options, and then deploy it to your client computers. See “Installing clients with Web Link and Email” on page 30. See “Installing clients with Remote Push” on page 36. See “Installing clients with Save Package” on page 32. **Note:** Symantec recommends that you also install the client on the computer that hosts Symantec Endpoint Protection Manager.

Table 1-9 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.

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

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: Symantec Endpoint Protection Manager requires full access to the system registry for installation and normal operation. To prepare a Windows Server 2003 computer on which you plan to remotely install Symantec Endpoint Protection Manager, you must first allow remote control on the computer. When you connect with Remote Desktop, you must also use a console session or shadow the console session in Remote Desktop.

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

To install Symantec Endpoint Protection Manager

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

   If you have a product disc, insert it into the optical drive. The installation should start automatically. If it does not start, open the disc, and then double-click **Setup.exe**.

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 management server 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 Symantec Endpoint Protection Manager during installation" on page 27.

8. You configure the management server according to your requirements. Follow the on-screen instructions to specify the type of configuration, the settings for the administrator and for mail server communications. You also choose whether to run LiveUpdate as part of the installation. If you run LiveUpdate as part of a new installation, content is more readily available for the clients you deploy.

   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 logon screen appears if you leave the option checked to launch Symantec Endpoint Protection Manager. Once you log in, you can begin client deployment.

See "Getting up and running on Symantec Endpoint Protection for the first time" on page 20.

Configuring Symantec Endpoint Protection Manager during installation

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

See "Installing Symantec Endpoint Protection Manager" on page 25.

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, which is **Default configuration** or **Custom configuration**. The wizard provides information about each type.
- Whether you want to use a recovery file.

  Note: If this installation is the 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 mail server name and port number.
- The Symantec Sales Partner information, if a partner 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 12.1.x 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 an additional paid license in response to an over-deployment status.
- Activating a license after you upgrade from a previous version, such as 11.0.

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 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 to step 3.

To activate or import your Symantec Endpoint Protection 12.1.x product license

1. In Symantec Endpoint Protection Manager, click **Admin > Licenses**.
2. Under **Tasks**, click **Activate license**.
3. Click **Activate a new license**, and then click **Next**. If you do not see this panel, continue to the next step.

4 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, you receive a Symantec license file (.slf file) 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 webpage:

Enterprise Options

5 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 came with your Symantec notification email. Click **Open**, and then click **Next**.

6 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.

7 Click **Finish**.

See "Getting up and running on Symantec Endpoint Protection for the first time" on page 20.

Installing clients with Web Link and Email

The Web Link and Email option creates the installation package and the URL for the installation package, and then sends the link to users in an email. The users download the package and install the Symantec Endpoint Protection client. Users must have administrator privileges to install the package.

Web Link and Email comprises the following tasks:

- You select, configure, and then create the client installation package.
  You choose from the options that appear for the configuration of Windows, Mac, and Linux client installation packages. All client installation packages are stored on the computer that runs Symantec Endpoint Protection Manager.
- Email from Symantec Endpoint Protection Manager notifies the computer users that they can download the client installation package.
  You provide a list of users to receive an email message, which contains instructions to download and install the client installation package. Users follow the instructions to install the client software.

Note: The Mac and the Linux client install packages automatically export a `.zip` archive file format. To correctly preserve the file permissions, you should expand the archive file with a native archive program, such as 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 the files for these operating systems.

Before you begin the client installation with Web Link and Email, make sure that you correctly configure the connection from the management server to the mail server.

To install clients with 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**, and then click **Next**. Web Link and Email only sends a new installation package.
3. Make selections from the available options, which vary depending on the installation package type, and then click **Next**.

   Note: To uninstall third-party security software on the Windows 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 About the third-party security software removal feature in Symantec Endpoint Protection 12.1.

   See "How Symantec Endpoint Protection uses layers to protect computers" on page 14.
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 and secure online location, like an intranet page.
6. To create the package and deliver the link by email, click **Next**, and then click **Finish**.
7. 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 restart. Depending on the client restart settings of the installed client, you or the computer users may need to restart the client computers. Mac clients prompt a restart when installation completes. Linux clients do not require a restart.

Installing clients with Save Package

Save Package creates the installation packages that you can install either manually, with third-party deployment software, or with a login script.

Save Package comprises the following tasks:

- You make your configuration selections and then create the client installation packages.
- You save the installation package to a folder on the computer that runs Symantec Endpoint Protection Manager.
  For Windows, the installation package can be for 32- or 64-bit operating systems. The installation package comprises one setup.exe file or a collection of files that includes a setup.exe file. Computer users often find one setup.exe file easier to use.

Either you or the end user can install the installation package on the client computer. Alternately, you can use third-party deployment software to perform the installation.

To install clients with Save Package

1. In the console, on the **Home** page, in the **Common Tasks** menu, click **Install protection client to computers**.
2. In the **Client Deployment Wizard**, do one of the following tasks:
   - Click **New Package Deployment**, and then click **Next**. Save Package only installs a new installation package.
   - Click **Communication Update Package Deployment** if you want to update Windows or Mac client communication settings on the computers that already have the Symantec Endpoint Protection client installed. Follow the on-screen instructions, and then go to step 4.
3. Make selections from the available options, which vary depending on the installation package type, and then click **Next**.

   Note: To uninstall third-party security software on the Windows 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 About the third-party security software removal feature in Symantec Endpoint Protection 12.1
4. Click **Save Package**, and then click **Next**.

5 Click **Browse** and specify the folder to receive the package.

For Communication Update Package Deployment, or for Mac and Linux packages, go to step 6.

For new Windows packages, check **Single .exe file (default)** or **Separate files (required for .MSI)**.

Note: Use **Single .exe file** unless you require separate files for a third-party deployment program.

6 Click **Next**.

7 Review the settings summary, click **Next**, and then click **Finish**.

8 Provide the exported package to the computer users.

For example, you can save the package to a secure shared network location, or email the package to the computer users. You can also use a third-party program to install the package.

9 Confirm that the user downloads and installs the client software, and confirm the installation status of the clients.

For new client installations, the client computers may not appear within the management console until after they restart. Depending on the client restart settings of the client, you or the computer users may need to restart the client computers. Mac clients prompt a restart when installation completes. Linux clients do not require a restart.

Installing the Symantec Endpoint Protection client for Mac

You can directly install an unmanaged or managed Symantec Endpoint Protection client on a Mac computer if you cannot use or do not want to use Remote Push. The steps are similar whether the client is unmanaged or managed.

The only way to install a managed client is with a package you create with Symantec Endpoint Protection Manager. You can convert an unmanaged client to a managed client at any time by importing client-server communication settings into the Mac client.

Note: To prepare the Symantec Endpoint Protection client for Mac for use with third-party remote deployment software, see Exporting and Deploying a Symantec Endpoint Protection client via Apple Remote Desktop or Casper.

If you downloaded the installation file or received a product disc

1. Perform one of the following tasks:

   If you downloaded the installation file, extract the contents to a folder on a Mac computer, and then open the folder.

   If you received a disc, insert it into a computer.
2. Open `SEP_MAC`.
3. Copy `Symantec Endpoint Protection.dmg` to the desktop of the Mac computer.
4. Double-click `Symantec Endpoint Protection.dmg` to mount the file as a virtual disk. You then install the Symantec Endpoint Protection client for Mac.

If you have a client installation package .zip

1. If you exported the installation package or downloaded the client installer package from FileConnect, copy the file to the desktop of the Mac computer.

   The file may be named `Symantec Endpoint Protection.zip` or `Symantec_Endpoint_Protection_`*`version`*`_Mac_Client.zip`, where *version* is the product version.
2. Right-click **Open With > Archive Utility** to extract the file's contents.
3. Open the resulting folder. You then install the Symantec Endpoint Protection client for Mac.

Note: The resulting virtual disk image or folder contains the application installer and a folder called **Additional Resources**. Both items must be present in the same location for a successful installation. If you copy the installer to another location, you must also copy **Additional Resources**.

To install the Symantec Endpoint Protection client for Mac

1. Double-click **Symantec Endpoint Protection Installer**.
2. To acknowledge the required restart, click **Continue**.
3. To review the license agreement, click **View License Agreement**.

   To begin the installation, click **Agree & Install**.

4 Enter the user name and password for the Mac administrative account when prompted, and then click **Install Helper**.

5 Click **Close & Restart** to complete the installation.

When you log back on to the Mac computer, LiveUpdate launches to update the definitions. LiveUpdate runs silently in the background, and does not display its progress onscreen.

See "Installing clients with Save Package" on page 32.

See "Installing clients with Remote Push" on page 36.

Installing the Symantec Endpoint Protection client for Linux

You install an unmanaged or managed Symantec Endpoint Protection client directly on a Linux computer. You cannot deploy the Linux client from Symantec Endpoint Protection Manager remotely. The installation steps are similar whether the client is unmanaged or managed.

The only way to install a managed client is with an installation package that you create in Symantec Endpoint Protection Manager. You can convert an unmanaged client to a managed client at any time by importing client-server communication settings into the Linux client.

Note: You must have superuser privileges to install the Symantec Endpoint Protection client on the Linux computer. The procedure uses `sudo` to demonstrate this elevation of privilege.

To install the Symantec Endpoint Protection client for Linux

1 Copy the installation package that you created to the Linux computer. The package is a .zip file.

2 On the Linux computer, open a terminal application window.

3 Navigate to the installation directory with the following command:

```
cd /directory/
```

Where *directory* is the name of the directory into which you copied the .zip file.

4 Extract the contents of the .zip file into a directory named `tmp` with the following command:

`unzip "InstallPackage" -d sepfiles`

Where *`InstallPackage`* is the full name of the .zip file, and *`sepfiles`* represents a destination folder into which the extraction process places the installation files.

If the destination folder does not exist, the extraction process creates it.

5 Navigate to *`sepfiles`* with the following command:

`cd sepfiles`

6 To correctly set the execute file permissions on `install.sh`, use the following command:

`chmod u+x install.sh`

7 Use the built-in script to install Symantec Endpoint Protection with the following command:

`sudo ./install.sh -i`

Enter your password if prompted.

This script initiates the installation of the Symantec Endpoint Protection components. The default installation directory is as follows:.

`/opt/Symantec/symantec_antivirus`

The default work directory for LiveUpdate is as follows:

`/opt/Symantec/LiveUpdate/tmp`

The installation completes when the command prompt returns. You do not have to restart the computer to complete the installation.

To verify the client installation, click or right-click the Symantec Endpoint Protection yellow shield and then click **Open Symantec Endpoint Protection**. The location of the yellow shield varies by Linux version. The client user interface displays information about program version, virus definitions, server connection status, and management.

Installing clients with Remote Push

Remote Push pushes the client software to the computers that you specify. Using Remote Push requires knowledge of how to search networks to locate computers by IP address or computer names. Once the package copies to the target computer,

the package installs automatically. The computer user does not need to begin the installation or to have administrator privileges.

Remote Push comprises the following tasks:

- You select an existing client installation package, create a new installation package, or create a package to update communication settings.
- For new installation packages, you configure and create the installation package.
- You specify the computers on your network to which Symantec Endpoint Protection Manager sends a package.
  Remote Push locates either specific computers for which you provide an IP number or range, or all computers that are visible by browsing the network.

  Note: To push the client installation package to Mac clients in the **Browse Network** tab, you must install the Bonjour service on the Symantec Endpoint Protection Manager server. See the following Knowledge Base article:

  Installing the Bonjour Service for Symantec Endpoint Protection Manager 12.1.5

- Symantec Endpoint Protection Manager pushes the client software to the specified computers.
  The installation automatically begins on the computers once the package successfully copies to the target computer.

Note: You cannot install the Linux client with Remote Push.

To install clients with Remote Push

1. In the console, on the **Home** page, in the **Common Tasks** menu, click **Install protection client to computers**.
2. In the **Client Deployment Wizard**, do one of the following tasks:
   - Click **New Package Deployment** to create a new installation package, and then click **Next**.
   - Click **Existing Package Deployment** to use a package that was previously created, and then click **Browse** to locate the package to install.
     The Client Deployment Wizard uploads the package and directs you to the **Computer Selection** panel (step 5).
   - Click **Communication Update Package Deployment** if you want to update Windows or Mac client communication settings on the computers that already have the Symantec Endpoint Protection client installed. Follow the on-screen instructions, and then go to step 4.

Use this option to convert an unmanaged client to a managed client.

3 For a new package, in the **Select Group and Install Feature Sets** panel, make selections from the available options, which vary depending on the installation package type. Click **Next**.

To uninstall third-party security software on the Windows client, you must configure custom Client Install Settings before you launch the Client Deployment Wizard. You can also use an existing client install package that is configured to enable this function. To see which third-party software the client package removes, see About the Security Software Removal feature in Symantec Endpoint Protection 12.1.

4 Click **Remote Push**, and then click **Next**.

5 In the **Computer Selection** panel, locate the computers to receive the software using one of the following methods:

- To browse the network for computers, click **Browse Network**.
- To find computers by IP address or computer name, click **Search Network**, and then click **Find Computers**.

You can set a timeout value to constrain the amount of time that the server applies to a search.

6 Click **> >** to add the computers to the list, and authenticate with the domain or workgroup if the wizard prompts you.

The remote push installation requires elevated privileges. If the client computer is part of an Active Directory domain, you should use a domain administrator account.

7 Click **Next**, and then click **Send** to push the client software to the selected computers.

Once the **Deployment Summary** panel indicates a successful deployment, the installation starts automatically on the client computers.

The installation takes several minutes to complete.

8 Click **Next**, and then click **Finish**.

9 Confirm the status of the installed clients on the **Clients** page.

For new Symantec Endpoint Protection installations, the client computers may not appear within the management console until after they are restarted. Depending on the client restart settings of the client, you or the computer users may need to restart the client computers.

Testing Symantec Endpoint Protection Manager policies

You may need to evaluate Symantec Endpoint Protection or you may need to test the policies before you download them to the client computers. You can test the following functionality using the Symantec Endpoint Protection Manager policies to make sure the product works correctly on the client computers.

Table 1-10 Features that you can test

Feature	See this topic
Virus and Spyware Protection	To test a default Virus and Spyware Protection policy, download the EICAR test virus from: http://www.eicar.org/86-0-Intended-use.html Testing a Virus and Spyware Protection policy
SONAR	Download the Socar.exe test file to verify that SONAR works correctly
Insight	How to test connectivity with Insight and Symantec Licensing servers
Intrusion Prevention	Testing a default IPS policy
Application Control	Blocking a process from starting on client computers Preventing users from writing to the registry on client computers Preventing users from writing to a particular file Adding and testing a rule that blocks a DLL Adding and testing a rule that terminates a process

Where to get more information

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

Table 1-11 Symantec websites

Types of information	Web address
Trial versions	Trialware

Table 1-11 Symantec websites *(continued)*

Types of information	Web address
Manuals and documentation updates	■ Product guides for all versions of Symantec Endpoint Protection and Symantec Endpoint Protection Small Business Edition (English) ■ Symantec Endpoint Protection (other languages) ■ Symantec Endpoint Protection Small Business Edition (other languages) ■ Product guides for all versions of Symantec Network Access Control (English) ■ Symantec Network Access Control (other languages)
Technical Support	Includes the public knowledge base, product release details, updates and patches, and contact options for support. Endpoint Protection Technical Support Endpoint Protection Small Business Edition Symantec Network Access Control
Virus and other threat information and updates	Security Response
Free online technical training	SymantecTV
Symantec Educational Services	Symantec Endpoint Security Training Courses
Symantec Connect forums	Endpoint Protection (AntiVirus) Endpoint Protection Small Business Edition 12.x Network Access Control