Symantec™ Endpoint Protection Small Business Edition Getting Started Guide

Symantec Endpoint Protection Small Business Edition Getting Started Guide

Documentation version: 12.01.00.00

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 Small Business Edition

This document includes the following topics:

- About Symantec Endpoint Protection Small Business Edition
- About the types of threat protection that Symantec Endpoint Protection Small Business Edition provides
- Components of Symantec Endpoint Protection Small Business Edition
- What's new in version 12.1
- System requirements
- Getting up and running on Symantec Endpoint Protection Small Business Edition for the first time
- Installing the management server and the console
- Activating your product license
- Deploying clients using a Web link and email
- Where to get more information

About Symantec Endpoint Protection Small Business Edition

Symantec Endpoint Protection Small Business Edition is a client-server solution that protects laptops, desktops, 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 Small Business Edition communicates over your network to automatically safeguard computers against attacks for both physical systems and virtual systems.

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 and the single client.

Symantec Endpoint Protection Small Business Edition Small Business Edition incorporates many of the features from the enterprise edition. It is designed for small-to-medium businesses with up to 250 clients.

See "About the types of threat protection that Symantec Endpoint Protection Small Business Edition provides" on page 4.

About the types of threat protection that Symantec Endpoint Protection Small Business Edition provides

Symantec Endpoint Protection Small Business Edition uses state-of-the-art protection to integrate multiple types of protection on each computer in your network. It offers advanced defense against all types of attacks for both physical systems and virtual systems. You need combinations of all the protection technologies to fully protect and customize the security in your environment. Symantec Endpoint Protection Small Business Edition combines traditional scanning, behavioral analysis, intrusion prevention, and community intelligence into a superior security system.

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

Table 1-1 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. ■ Symantec Insight provides faster and more accurate malware detection to detect the new and the unknown threats that other approaches miss. Insight identifies new and zero-day threats by using the collective wisdom of over millions of systems in hundreds of countries. ■ Bloodhound uses heuristics to detect a high percentage of 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 intrusion prevention protection 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 shields computers from malicious threats before they appear. ■ The IPS scans network traffic and files for indications of intrusions or attempted intrusions. ■ Browser Intrusion Prevention scans for attacks that are directed at browser vulnerabilities. ■ Universal download protection monitors all downloads from the browser and validates that the downloads are not malware.

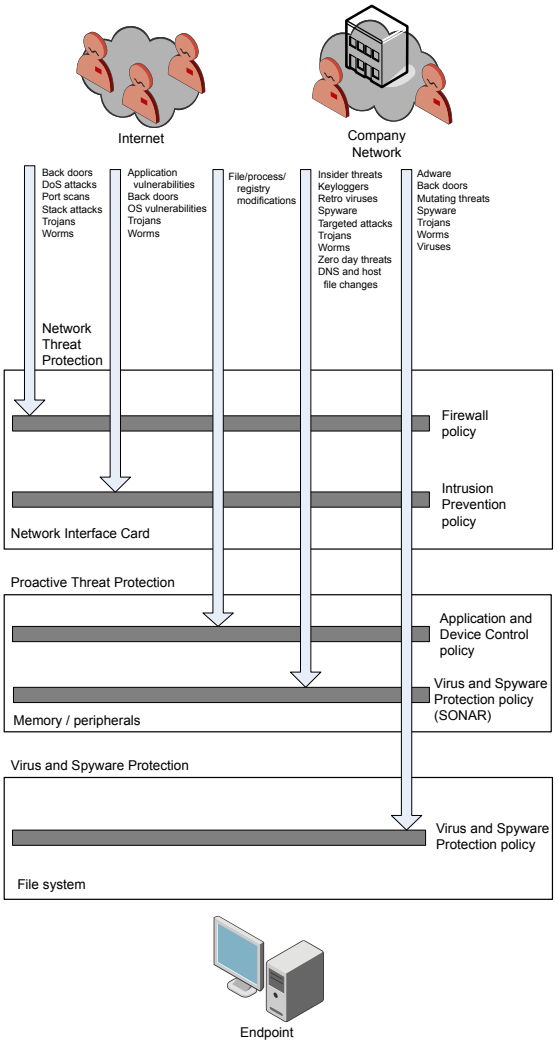
Table 1-1 Layers of protection *(continued)*

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.	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.

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



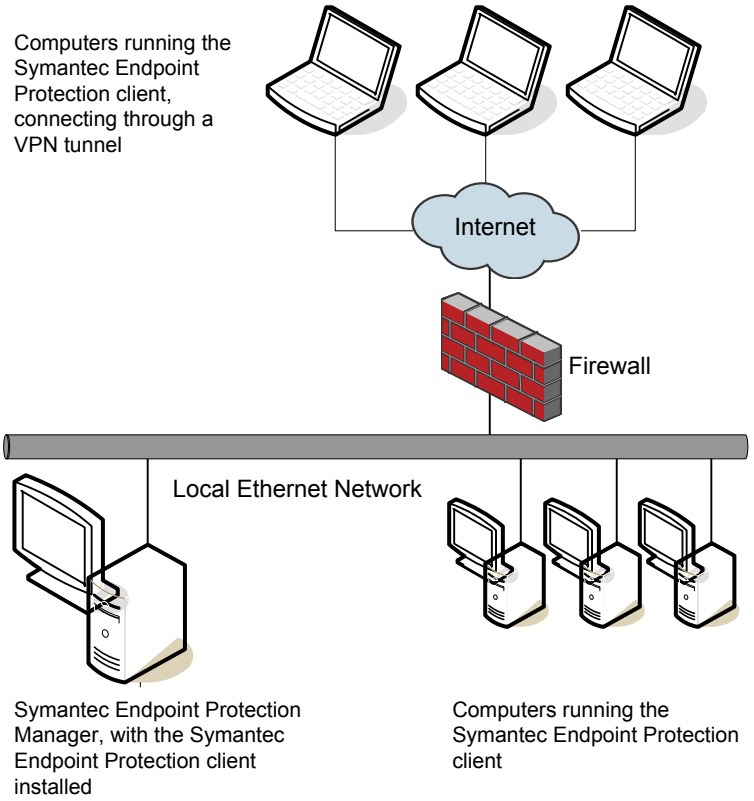
Components of Symantec Endpoint Protection Small Business Edition

Table 1-2 lists the product's components and describes their functions.

Table 1-2 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 software: ■ The console software coordinates and manages security policies, client computers, reports, and logs. The console is the interface to the management server. It can also be installed and used remotely on any computer with a network connection to the management server. ■ The management server software provides secure communication to and from the client computers and the console.
Database	The database stores security policies and events. The database is installed on the computer that hosts Symantec Endpoint Protection Manager.
Symantec Endpoint Protection Small Business Edition client	The Symantec Endpoint Protection Small Business Edition client protects the 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, see the *Symantec Endpoint Protection Small Business Edition Client Guide*. See "About Symantec Endpoint Protection Small Business Edition" on page 4.

Figure 1-2 The product components in a network



See "About the types of threat protection that Symantec Endpoint Protection Small Business Edition provides" on page 4.

What's new in version 12.1

The current release includes the following improvements that make the product easier and more efficient to use.

Table 1-3 displays the new features in version 12.1.

Table 1-3 New features in version 12.1

Feature	Description

Better security against malware	The most significant improvements include the following policy features to provide better protection on the client computers.
	■ The Virus and Spyware Protection policy detects threats more accurately while it reduces false positives and improves scan performance with the following technologies:
	  ■ SONAR replaces the TruScan technology to identify malicious behavior of unknown threats using heuristics and reputation data. While TruScan runs on a schedule, SONAR runs at all times.
	  ■ Auto-Protect provides additional protection with Download Insight, which examines the files that users try to download through Web browsers, text messaging clients, and other portals. Download Insight uses reputation information from Symantec Insight to make decisions about files.
	  ■ Insight lets scans skip Symantec and community trusted files, which improves scan performance.
	  ■ Insight Lookup detects the application files that might not typically be detected as risks and sends information from the files to Symantec for evaluation. If Symantec determines that the application files are risks, the client computer then handles the files as risks. Insight Lookup makes malware detection faster and more accurate.
	■ The Firewall policy includes firewall rules to block IPv6-based traffic.
	■ The Intrusion Prevention policy includes browser intrusion prevention, which uses IPS signatures to detect the attacks that are directed at browser vulnerabilities.

Faster and more flexible management	Symantec Endpoint Protection Manager helps you manage the client computers more easily with the following new features: ■ Centralized licensing lets you purchase, activate, and manage product licenses from the management console. ■ The Symantec Endpoint Protection Manager logon screen enables you to have your forgotten password emailed to you. ■ The **Monitors** page includes a set of preconfigured email notifications that inform you of the most frequently used events. The events include when new client software is available, when a policy changes, license renewal messages, and when the management server locates unprotected computers. The notifications are enabled by default and support the BlackBerry, iPhone, and Android. ■ Improved status reporting automatically resets the **Still Infected Status** for a client computer once the computer is no longer infected.

Table 1-3 New features in version 12.1 *(continued)*

Feature	Description
Better server and client performance	To increase the speed between the management server and the management console, database, and the client computers: ■ Virus and spyware scans use Insight to let scans skip safe files and focus on files at risk. Scans that use Insight are faster and more accurate, and reduce scan overhead by up to 70 percent. ■ LiveUpdate can run when the client computer is idle, has outdated content, or has been disconnected, which uses less memory.
Support for Mac clients	In Symantec Endpoint Protection Small Business Edition, you can now deploy and manage Mac clients in Symantec Endpoint Protection Manager. See "Deploying clients using a Web link and email" on page 18.
Improved installation process	You can install the product faster and easier than before with the following new installation features: ■ You can upgrade to the current version of the product while the legacy clients stay connected and protected. ■ A new quick report for deployment shows which computers have successfully installed the client software.
Support for additional operating systems	Symantec Endpoint Protection Manager now supports the following additional operating systems: ■ VMware Workstation 7.0 or later ■ VMware ESXi 4.0.x or later ■ VMware ESX 4.0.x or later ■ VMware Server 2.0.1 ■ Citrix XenServer 5.1 or later Symantec Endpoint Protection Manager now supports the following Web browsers: ■ Internet Explorer 7.0, 8.0, 9.0 ■ Firefox 3.6, 4.0 See "System requirements" on page 12.

For more information, see the *Symantec Endpoint Protection Small Business Edition Implementation Guide*.

System requirements

In general, the system requirements for Symantec Endpoint Protection Manager and the clients are the same as those of the supported operating systems. Additional details are provided in the following tables.

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

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

Table 1-4 Symantec Endpoint Protection Manager system requirements

Component	Requirements
Processor	■ 32-bit processor: 1-GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended) ■ 64-bit processor: 2-GHz Pentium 4 with x86-64 support or equivalent minimum **Note:** Intel Itanium IA-64 and PowerPC 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
Display	800 x 600
Operating system	■ Windows 7 ■ Windows XP (32-bit, SP3 or later; 64-bit, all SPs) ■ Windows Server 2003 (32-bit, 64-bit, R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-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, or 9 ■ Mozilla Firefox 3.6 or 4.0

Note: Clients before version 12.1 can be managed by this version of the Symantec Endpoint Protection Manager, regardless of the client operating system.

Table 1-5 Symantec Endpoint Protection Small Business Edition 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 ■ 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	512 MB of RAM, or higher if required by the operating system
Hard drive	Hard disk: 700 MB or more free space
Display	800 x 600
Operating system	■ Windows XP (32-bit, SP2 or later; 64-bit, all SPs) ■ Windows XP Embedded ■ Windows Vista (32-bit, 64-bit) ■ Windows 7 (32-bit, 64-bit) ■ Windows Server 2003 (32-bit, 64-bit, R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-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 10.5 or 10.6 (32-bit, 64-bit) ■ Mac OS X Server 10.5 or 10.6 (32-bit, 64-bit)

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

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

Table 1-6 lists the tasks you should perform to install and protect the computers in your network immediately.

Table 1-6 Tasks to install and configure Symantec Endpoint Protection Small Business Edition

Action	Description
Install 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 the management server and the console" on page 17.
Create groups	You can add the 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.
Modify the Virus and Spyware Protection policy	Change the following default scan settings: ■ For the servers group, change the scheduled scan time to a time when most users are offline.
Activate the product license	Purchase and activate a license within 30 days of product installation. See "Activating your product license" on page 18.
Prepare computers for client installation (optional)	Before you install the client software, perform the following tasks, if necessary: ■ Uninstall third-party virus protection software from your computers. For more information on a tool to uninstall any competitive product automatically, see the knowledge base article, SEPprep competitive product uninstall tool. ■ 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 with the Client Deployment Wizard	Deploy the client software. See "Deploying clients using a Web link and email" on page 18.

Table 1-6 Tasks to install and configure Symantec Endpoint Protection Small Business Edition *(continued)*

Action	Description
Check that the computers are listed in the groups that you expected and that the client communicates with the management server	In the management console, on the **Computers** > **Computers** 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 **Computer** 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 the client last communicated with the management server. ■ The **Restart Required** column displays which 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. 2 Change to the **Protection technology** view and ensure that the following protections are **On**: ■ **Antivirus status** ■ **Firewall 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.
Check the LiveUpdate schedule and adjust if necessary	Make sure that the content updates download to client computers at a time that affects users the least.
Configure Symantec Endpoint Protection Manager to send email alerts	Alerts and notifications are critical to maintaining a secure environment and can also save you time.
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, do the following: 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**.

Table 1-7 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 1-7 Tasks to perform two weeks after you install

Action	Description
Exclude applications and files from being scanned	You can increase performance so that the client does not scan certain folders and files. For example, the client scans the mail server every time a scheduled scan runs. You can also exclude files by extension for Auto-Protect scans.
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.

For information on how to perform these tasks, see the *Symantec Endpoint Protection Small Business Edition Implementation Guide*.

Configuring the management server during installation

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

See "Installing the management server and the console" on page 17.

You can also start the Management 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:

- 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.

Installing the management server and the console

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

See "System requirements" on page 12.

See "Getting up and running on Symantec Endpoint Protection Small Business Edition for the first time" on page 13.

To install the management server and the console

1. If you have physical media, 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, unzip the folder and extract the entire product disc image to a physical disc, such as a hard disk. Run `Setup.exe` from the physical disc.

2. Click **Install**. On the sub-menu that is displayed, click **Install Symantec Endpoint Protection Manager**.

3. Review the sequence of installation events and click **Next**.

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 with the installation of the Symantec Endpoint Protection Manager and console. This part of the installation completes automatically.

7. In the installation summary panel, click **Next**.

   The **Management Server Configuration Wizard** starts automatically.

8. You configure the management server according to your requirements and then click **Next**.

   See "Configuring the management server during installation" on page 16.

9 In the **Symantec AntiVirus Migration** (optional) panel, click **No** if you do not need to migrate from Symantec AntiVirus or Symantec Client Security.

10 The Client Deployment Wizard starts automatically. You can deploy client software at any time. You can safely cancel client deployment if you do not want to deploy client software at this time.

See "Deploying clients using a Web link and email" on page 18.

Activating your product license

Activating a license saves the license file in the Symantec Endpoint Protection Manager database.

You can activate the following types of licenses:

- Paid licenses
- License renewal
- License for over-deployed clients

You can 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

To activate a license

1 In the console, click **Admin**, and then click **Licenses**.

2 Under **Tasks**, click **Activate license**.

3 Follow the instructions in the **License Activation Wizard** to complete the activation process.

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.

You perform this procedure in two stages:

- Select and configure 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.

- Notify 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` file. To expand the package to the Apple install format .mpkg, you must use either the Mac `Archive` Utility or the `ditto` command. You cannot use either the Mac unzip command or any Windows unzip application.

To deploy clients by using a Web link and email

1. On the **Home** page, in the **Common Tasks** menu, select **Install protection client to computers**.
2. Select the type of deployment you want to use and then click **Next**.

   The **New Package Deployment** option uses the packages that are stored on the Symantec Endpoint Protection Manager. By default, two packages are available. You can optionally create new packages with custom settings and features. **Existing Package Deployment** lets you use the packages that have been exported previously.
3. For a new package, select the package, the group, the installation feature set and content options and then click **Next**.

   The management server includes preconfigured packages.
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, and then click **Next**.

   You can either specify who receives the URL by email, or copy the URL and post it to a convenient online location. To specify multiple email recipients, type a comma after each email address.
6. If you want to deliver the link in email, accept the default email subject and body or edit the text, and then click **Next**.
7. Click **Finish**.
8. You or the computer users must restart the client computers.
9. Confirm that the computer users received the email message and installed the client software.

Where to get more information

The product includes several sources of information.

The primary documentation is available in the Documentation folder on the product disc. Updates to the documentation are available from the Symantec Technical Support Web site.

The product includes the following documentation:

- *Symantec Endpoint Protection Small Business Edition Implementation Guide*
  This guide includes procedures to install, configure, and manage the product.
- *Symantec Endpoint Protection Small Business Edition Client Guide*
  This guide includes procedures for users to use and configure the Symantec Endpoint Protection Small Business Edition client.
- *Symantec Client Firewall Policy Migration Guide*
  This guide explains how to migrate from Symantec Client Firewall Administrator to Symantec Endpoint Protection Manager.
- Online Help for Symantec Endpoint Protection Manager and Online Help for the client
  These Online Help systems contain the information that is in the guides plus context-specific content.
- Tool-specific documents that are located in the subfolders of the `Tools` folder on the product disc.

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 Small Business Edition 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=55357
Virus and other threat information and updates	http://www.symantec.com/business/security_response/index.jsp
Product news and updates	http://enterprisesecurity.symantec.com

Table 1-8 Symantec Web sites *(continued)*

Types of information	Web address
Free online technical training	http://go.symantec.com/education_septc
Symantec Educational Services	http://go.symantec.com/education_sep
Symantec Connect forums	http://www.symantec.com/connect/security/forums/endpoint-protection-small-business