

Symantec™ Endpoint Protection Getting Started Guide



Symantec™ Endpoint Protection Getting Started Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 11.00.04.00.00

PN: 20000329

Legal Notice

Copyright © 2008 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, LiveUpdate, Sygate, Symantec AntiVirus, Bloodhound, Confidence Online, Digital Immune System, Norton, 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.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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
20330 Stevens Creek Blvd.
Cupertino, CA 95014

<http://www.symantec.com>

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/techsupp/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system

- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

Asia-Pacific and Japan	contractsadmin@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Getting Started

This document includes the following topics:

- About Symantec Endpoint Protection
- What's included with Symantec Endpoint Protection
- What's new in this version
- Process for installing the product
- Post-installation tasks
- System requirements
- About installing for the first time
- About migrating to Symantec Endpoint Protection
- Installing and configuring the Symantec Endpoint Protection Manager with an embedded database
- Configuring and deploying client software
- Logging on to the Symantec Endpoint Protection Manager Console
- Adding a group
- About policies
- Configuring LiveUpdate for site updates
- About LiveUpdate policies for client updates
- Configuring a LiveUpdate Settings Policy
- Configuring a LiveUpdate Content Policy
- Configuring and testing Symantec Endpoint Protection

- Where to get more information about Symantec Endpoint Protection and Symantec Network Access Control

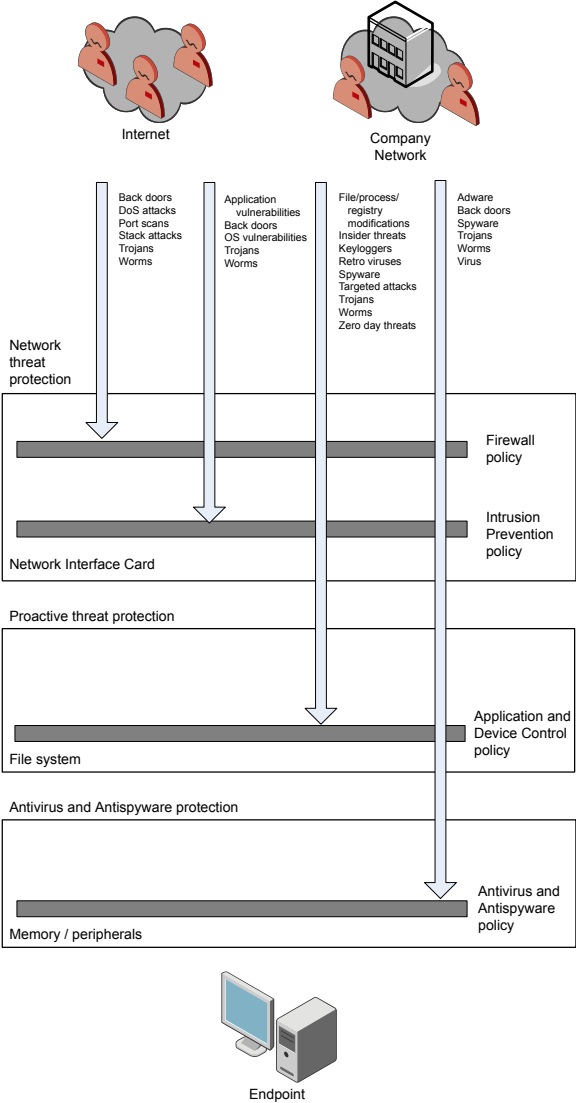
About Symantec Endpoint Protection

Symantec Endpoint Protection is the next-generation product that replaces specific versions of the following products:

- Symantec AntiVirus Corporate Edition
- Symantec Client Security
- Symantec Sygate Enterprise Protection
- Sygate Secure Enterprise
- Symantec WholeSecurity Confidence Online for Corporate PCs

Symantec Endpoint Protection provides advanced threat protection that protects your endpoints (laptops, desktops, and servers) from both known threats and those threats that have not been seen before. 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. Symantec Endpoint Protection also allows you to maintain fine-grained application and device control. Symantec Endpoint Protection provides multiple layers of protection for your endpoint computing devices.

Figure 1-1 Multiple protection layers



Symantec Network Access Control, which is purchased separately, is a companion product to Symantec Endpoint Protection. Symantec Network Access Control ensures that clients are compliant with your organization’s security policies before they are allowed access to your network.

What's included with Symantec Endpoint Protection

Symantec Endpoint Protection includes the following core components:

- The Symantec Endpoint Protection client is installed on the endpoints that you want to protect. It combines antivirus, antispymware, firewall, intrusion prevention system, application control, device control, and TruScan proactive threat scanning into a single client.

It also contains Symantec Network Access Control, which remains dormant until activated. No redeployment of clients is needed to add Symantec Network Access Control to a network where Symantec Endpoint Protection is installed. An update to the Symantec Endpoint Protection Manager activates those features on the clients.

- Symantec Endpoint Protection Manager is installed on a computer that you want to host the management server software. Symantec Endpoint Protection Manager communicates with the Symantec Endpoint Protection clients and is configured through the Symantec Endpoint Protection Manager Console.
- Symantec Endpoint Protection Manager Console lets you centrally manage the Symantec Endpoint Protection clients. From the console you can install clients, set and enforce a security policy, and monitor and report on the clients. The console can be run from the computer that hosts the Symantec Endpoint Protection Manager or remotely, by using a Web browser.

Larger companies may want to install the following optional components to centralize resources within the corporate network:

- The LiveUpdate Server, also known as Central LiveUpdate Server, obtains security and product updates from Symantec and acts as a repository for those updates. Symantec Endpoint Protection Manager and Symantec Endpoint Protection clients can be configured to retrieve updates from this LiveUpdate Server.
- The Central Quarantine receives suspicious files and unrepaired infected items from the Symantec Endpoint Protection clients. Central Quarantine forwards a sample to Symantec Security Response, which analyzes the sample. If a threat is new, Symantec Security Response produces security updates.

What's new in this version

Symantec Endpoint Protection combines technologies from previous Symantec products into a single new interface.

The Symantec Endpoint Protection client provides the following essential threat protection technologies.

Antivirus and Antispyware Protection	Adds rootkit detection and removal and has an improved resource footprint.
Network Threat Protection	Provides a rules-based firewall and an intrusion prevention system to prevent intrusion attacks and malicious content from reaching the client computer.
Proactive Threat Protection	Adds protection for zero-day attacks without relying on signatures. It also provides a way to block or limit processes or hardware devices on client computers.
Customizable interface	Administrators can control the configuration options that are available to the end user. They can also completely hide the interface.

Symantec Endpoint Protection is Symantec Network Access Control-ready with the purchase of Symantec Network Access Control.

The redesigned management console can be used to perform the following tasks:

- Manage both Symantec Endpoint Protection and Symantec Network Access Control. You can manage all security technologies from a single console.
- Monitor and report on security threats and system response from a central point.
- Give administrators access to the console that is based on their roles and responsibilities. For example, you can allow an administrator to manage only certain policy types.

Administrators for legacy Symantec AntiVirus Corporate Edition and Symantec Client Security products should see the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

The current release includes improvements that make Symantec Endpoint Protection and Symantec Network Access Control easier and more efficient to use.

Table 1-1 New features in this version

Feature	Benefit
<p>Symantec Endpoint Protection Manager now supports the following operating systems:</p> <ul style="list-style-type: none"> ■ Microsoft Windows Server 2008 (Standard/Enterprise/Datacenter/Web editions) ■ Microsoft Windows 2008 Small Business Server (Standard/Premium editions) ■ Microsoft Windows 2008 Essential Business Server (Standard/Premium editions) 	<p>Your company can now support new operating systems.</p>
<p>The client now supports the Microsoft Windows 2008 Small Business Server and Microsoft Windows 2008 Essential Business Server (Standard/Premium editions), for both the 32-bit and 64-bit versions.</p>	<p>Your company can protect the computers that run these new operating systems.</p>
<p>The Symantec Endpoint Protection Manager resumes downloads for maintenance releases and patches if a download is interrupted or stopped.</p>	<p>You can provide maintenance release updates and patches more efficiently.</p>
<p>The Group Update Provider includes the ability to configure the traffic bandwidth.</p>	<p>You can configure the time that is needed to download content to the Symantec Endpoint Protection Manager.</p>

For more detailed information about maintenance releases, you can read the release notes and additional post-release information at the following URL:

<http://www.symantec.com/business/support/overview.jsp?pid=54619>

Process for installing the product

The information in this section is specific to installing the product on a computer on which a version is not already installed.

Table 1-2 Process for installing the product

Step	Action	Description
Step 1	Review system and installation requirements	<p>Confirm that your network and the computers you plan to use meet the requirements to install and run the software.</p> <p>See “System requirements” on page 15.</p>
Step 2	Plan and prepare for the installation	<p>Decide which type of database to use, plan your deployment, and prepare client computers.</p> <p>See “About installing for the first time” on page 19.</p>
Step 3	Install Symantec Endpoint Protection Manager	<p>Run the installation program from the product disc. The program first installs the manager software. It then configures the management server and creates the database. Follow the procedure that corresponds to the type of database you select.</p> <p>See “Installing and configuring the Symantec Endpoint Protection Manager with an embedded database” on page 20.</p>
Step 4	Create and deploy a client installation package	<p>After you configure the database, you are asked if you want to run the Migration and Deployment Wizard. This wizard creates and then pushes out a default client software installation package.</p> <p>Alternately, you can:</p> <ul style="list-style-type: none"> ■ Use the Migration and Deployment Wizard from the Start menu at any time. ■ Create and deploy client software at a later time using the Find Unmanaged Computers utility in the console. <p>For more information, see the <i>Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control</i>.</p> <p>See “Configuring and deploying client software” on page 23.</p>

Post-installation tasks

After you install Symantec Endpoint Protection Manager, you must perform the following steps to configure protection for the computers in your network.

You follow these steps in the first day after you install the product. You can test the configuration while you familiarize yourself with the product. After the test period is successful, you then configure the protection for all the client computers in the network

Table 1-3 Post-installation tasks

Step	Action	Description
Step 1	Log on to Symantec Endpoint Protection Manager Console	To log on, you can use the Start menu and the admin user name, with the password that you set during installation. See “Logging on to the Symantec Endpoint Protection Manager Console” on page 25.
Step 2	Locate or add groups	On the Clients page, the group that you created when you installed appears under View Clients. See “Adding a group” on page 25.
Step 3	Configure LiveUpdate for site updates Configure LiveUpdate for client updates	You need to configure LiveUpdate properties for the site that you installed. See “Configuring LiveUpdate for site updates” on page 26. After you configure the site, you need to configure a LiveUpdate Settings Policy and a LiveUpdate Content Policy (Symantec Endpoint Protection only) for your clients. See “About LiveUpdate policies for client updates” on page 27.

Table 1-3 Post-installation tasks (*continued*)

Step	Action	Description
Step 4	Configure and test the security policies on the client	At a minimum, you should configure and test an Antivirus and Antispyware Policy for your clients. You may also want to configure a Firewall Policy and policies for the other types of protection. See “Configuring and testing Symantec Endpoint Protection” on page 29.

System requirements

Symantec software requires specific protocols, operating systems and service packs, software, and hardware. All the computers to which you install Symantec software should meet or exceed the recommended system requirements for the operating system that is used.

The Getting Started guides contain summary information about system requirements. This information may be sufficient to install to a small network or test network. You should refer to the full system requirements before you install the product on a more complex network.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for full system requirements.

Table 1-4 summarizes the minimum requirements for the computer on which you install the Symantec Endpoint Protection Manager Console.

Table 1-4 Symantec Endpoint Protection Manager system requirements

Component	Requirement
Operating system	<p>32-bit systems:</p> <ul style="list-style-type: none"> ■ Windows 2000 Server/Advanced Server/Datacenter Server Editions, with Service Pack 3 or later ■ Small Business Server 2000 ■ Windows XP Professional Edition with SP 1 or later (x86 or x64) ■ Windows Server 2003 Web Edition ■ Windows Server 2003 Standard/Enterprise/Datacenter Editions (x86 or x64) ■ Windows Small Business Server 2003 ■ Windows Compute Cluster Server 2003 ■ Windows Storage Server 2003 ■ Windows Server 2008 Standard/Windows Server 2008 Enterprise/Windows Server 2008 Datacenter/Windows Web Server 2008 <p>64-bit systems:</p> <ul style="list-style-type: none"> ■ Windows Essential Business Server 2008 Standard Edition/Windows Essential Business Server 2008 Premium Edition ■ Windows Small Business Server 2008 Standard Edition/Windows Small Business Server 2008 Premium Edition
Database	<p>The Symantec Endpoint Protection Manager includes an embedded database.</p> <p>You can also use Microsoft SQL Server 2000 with SP3 or later, or Microsoft SQL Server 2005. SQL Server is optional.</p>
Other software	<ul style="list-style-type: none"> ■ Internet Information Services server 5.0 or later with Web services enabled. ■ Internet Explorer 6.0 or later ■ Static IP address recommended
Hardware	<ul style="list-style-type: none"> ■ 1 GB RAM (2-4 GB recommended) ■ 4 GB on the hard disk for the server, plus 4 GB for the database ■ VGA (640x480) or higher resolution video adapter and monitor

Table 1-5 summarizes the minimum requirements for the remote computer on which you run the Symantec Endpoint Protection Manager Console.

Table 1-5 Symantec Endpoint Protection Manager Console system requirements

Component	Requirement
Operating system	32-bit systems: <ul style="list-style-type: none">■ Windows 2000 with SP3 or later■ Windows XP■ Windows Server 2003■ Windows Vista 64-bit systems: <ul style="list-style-type: none">■ Windows Essential Business Server 2008 Standard Edition/Windows Essential Business Server 2008 Premium Edition■ Windows Small Business Server 2008 Standard Edition/Windows Small Business Server 2008 Premium Edition
Hardware	<ul style="list-style-type: none">■ 512 MB RAM, 1 GB recommended■ 15 MB hard drive■ VGA (640x480) or higher resolution video adapter and monitor

Table 1-6 summarizes the minimum requirements for the computers on which you install the client software for either Symantec Endpoint Protection or Symantec Network Access Control.

Table 1-6 Client software system requirements

Component	Requirement
Operating system	<p>32-bit systems:</p> <ul style="list-style-type: none"> ■ Windows 2000 Professional/Server/Advanced Server/Datacenter Server Editions, with SP 3 or later ■ Small Business Server 2000 ■ Windows XP Home/Tablet PC/Media Center Editions Windows XP Professional Edition /XP Embedded Edition (x86 or x64) ■ Windows Vista Home Basic Edition Windows Vista Home Premium/Business/Enterprise/Ultimate Editions (x86 or x64) ■ Windows Server 2003 Web Edition Windows Server 2003 Standard/Enterprise/Datacenter Editions (x86 or x64) ■ Windows Small Business Server 2003 ■ Windows Server 2008 Standard/Enterprise/ Datacenter Editions (x86 or x64) ■ Windows Web Server 2008 (x86 or x64) <p>64-bit systems:</p> <ul style="list-style-type: none"> ■ Windows Essential Business Server 2008 Standard Edition/Windows Essential Business Server 2008 Premium Edition ■ Windows Small Business Server 2008 Standard Edition/Windows Small Business Server 2008 Premium Edition
Other software	<p>Internet Explorer 6.0 or later</p> <p>Terminal Server clients connecting to a computer with antivirus protection have the following additional requirements:</p> <ul style="list-style-type: none"> ■ Microsoft Terminal Server RDP (Remote Desktop Protocol) client ■ Citrix Metaframe (ICA) client 1.8 or later if you use Citrix Metaframe server on Terminal Server
Hardware	<ul style="list-style-type: none"> ■ 256 MB RAM ■ 600 MB hard disk on 32-bit systems, 700 MB hard disk on 64-bit systems ■ VGA (640x480) or higher resolution video adapter and monitor

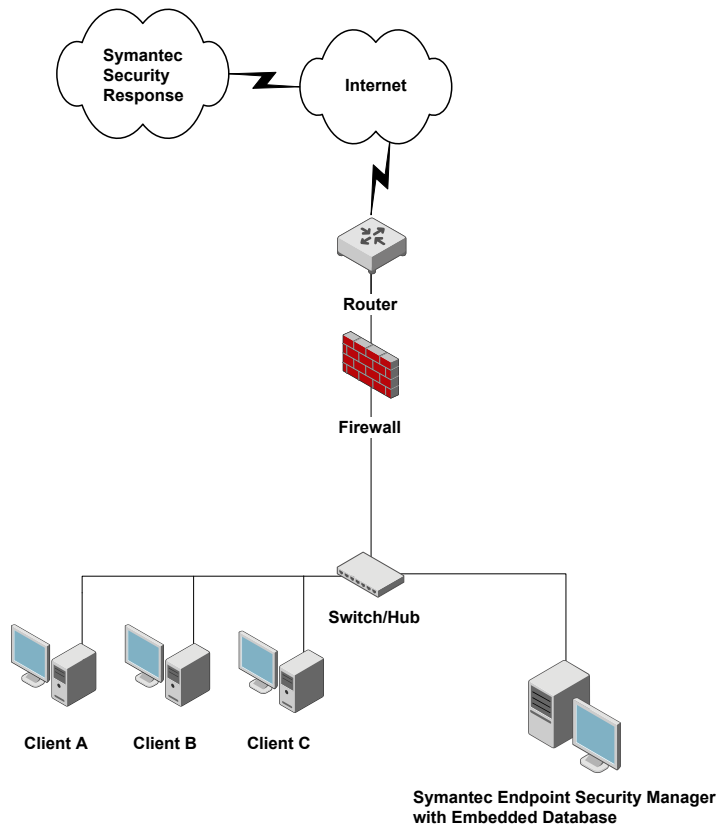
For information about using the Symantec AntiVirus client on Linux, see the *Symantec AntiVirus for Linux Client Guide*.

The guide is located in the docs folder of the product disc that contains the Symantec AntiVirus client software for Linux.

About installing for the first time

If this installation is a first-time installation, you should install, configure, and test Symantec Endpoint Protection or Symantec Network Access Control software in a test environment.

Figure 1-2 Sample test environment



This test environment contains three clients and one server. The server runs three management components. The three management components are Symantec Endpoint Protection Manager, Symantec Endpoint Protection Manager Console, and the embedded database. These installation and configuration procedures are designed for this sample test environment.

You must install Symantec Endpoint Protection Manager before you install the client software.

If you install the client software from the product disc, you install an unmanaged client.

About migrating to Symantec Endpoint Protection

You must perform a migration if you have installed on your network a migration-supported version of the following products:

- Symantec AntiVirus Corporate Edition
- Symantec Client Security
- Symantec Sygate Enterprise Protection
- Sygate Secure Enterprise

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

Installing and configuring the Symantec Endpoint Protection Manager with an embedded database

Installing with the embedded database is the easiest way to install Symantec Endpoint Protection Manager. The embedded database supports up to 5,000 clients. If you choose to configure the management server in Simple mode the embedded database is selected automatically.

The installation of Symantec Endpoint Protection Manager is divided into three parts:

- The first part installs the management server and console.
- The second part configures the server and creates the database.
- The third part creates and deploys client software to the client computers. You can deploy the client software during the management server installation or later.

Each part consists of a wizard. When the wizard for each part completes, a prompt is displayed asking you whether you want to continue with the next wizard or not.

To install Symantec Endpoint Protection Manager

- 1 Insert the product disc into the drive, and start the installation.
- 2 In the Welcome panel, do one of the following actions:
 - To install for Symantec Endpoint Protection, click **Install Symantec Endpoint Protection Manager**.

- To install for Symantec Network Access Control, click **Install Symantec Network Access Control**, and then click **Install Symantec Endpoint Protection Manager**.
- 3 On the Welcome pane of the Installation Wizard, click **Next**.

A check is performed to see if the computer meets the minimum system requirements. If it does not, a message indicates which resource does not meet the minimum requirements. You can click **Yes** to continue installing Symantec Endpoint Protection Manager, but performance can be adversely affected.
 - 4 In the License Agreement panel, check **I accept the terms in the license agreement**, and then click **Next**.
 - 5 In the Destination Folder panel, accept or change the installation directory, and then click **Next**.
 - 6 On the Select Web site panel, do one of the following:
 - To configure the Symantec Endpoint Protection Manager IIS Web as the only Web server on this computer, check **Create a custom Web site**, and then accept or change the **TCP Port**.
 - To let the Symantec Endpoint Protection Manager IIS Web server run with other Web sites on this computer, check **Use the default Web site**.
 - 7 Click **Next**.
 - 8 In the Ready to Install the Program panel, click **Install**.
 - 9 When the installation finishes and the Install Wizard Completed panel appears, click **Finish**.

Wait for the Management Server Configuration Wizard dialog box to appear, which can take several seconds. If you are prompted to restart the computer, restart the computer, log on, and the wizard appears automatically for you to continue.
 - 10 Follow the steps for the appropriate mode of configuration that you select: Simple or Advanced.

To configure the Symantec Endpoint Protection Manager with an embedded database in Simple mode

- 1 In the Management Server Configuration Wizard dialog box, select **Simple**, and then click **Next**.
- 2 Provide and confirm a password of 6 or more characters. Optionally, provide an administrator email address.

The password is the admin account password that you use to log on to the Symantec Endpoint Protection Manager Console. The password is also used as the encryption password necessary for disaster recovery and for adding optional Enforcers. After installation, the encryption password does not change, even if the password for the admin account is changed.

Document this password for when you install Symantec Endpoint Protection in your production environment.

- 3 Click **Next**.
- 4 The configuration summary panel displays the values that are used to install Symantec Endpoint Protection Manager. You can print a copy of the settings to maintain for your records, or click **Next**.

Wait while the installation creates the database, which can take several minutes.

- 5 In the Management Server Configuration Wizard Completed panel, do one of the following:
 - To deploy client software with the Migration and Deployment Wizard, click **Yes**, and then click **Finish**.
See “Configuring and deploying client software” on page 23.
 - To log on to the Symantec Endpoint Protection Manager Console first, and then deploy client software, click **No**, and then click **Finish**.
See “Logging on to the Symantec Endpoint Protection Manager Console” on page 25.

To configure the Symantec Endpoint Protection Manager with an embedded database in Advanced mode

- 1 In the Management Server Configuration Wizard dialog box, select **Advanced**, and then click **Next**.
- 2 Select the number of clients you want this server to manage, and then click **Next**.

This selection appears only when you install the Symantec Endpoint Protection Manager for the first time on this computer.

- 3 Check **Install my first site**, and then click **Next**.

- 4 In the server information panel, accept or change the default values, and then click **Next**.
- 5 In the site name panel, in the Site name box, accept or change the default name, and then click **Next**.
- 6 In the encryption password panel, provide and confirm a password, and then click **Next**.

Document this password and store it in a safe, secure location. You cannot change or recover the password after you create the database. You must also enter this password for disaster recovery purposes if you do not have a backed up database to restore.

- 7 In the database type panel, check **Embedded database**, and then click **Next**.
- 8 In the system administrator account panel, provide and confirm a password of 6 or more characters. Optionally, provide an administrator email address. Click **Next**.

Use the user name and password that you set here to log on to the console for the first time.

Wait while the installation creates the database, which can take several minutes.

- 9 In the Management Server Configuration Wizard Completed panel, do one of the following:
 - To deploy client software with the Migration and Deployment Wizard, click **Yes**, and then click **Finish**.
See “Configuring and deploying client software” on page 23.
 - To log on to the Symantec Endpoint Protection Manager Console first, and then deploy client software, click **No**, and then click **Finish**.
See “Logging on to the Symantec Endpoint Protection Manager Console” on page 25.

Configuring and deploying client software

The Migration and Deployment Wizard lets you configure a client software package. The Push Deployment Wizard then optionally appears to let you deploy the client software package.

Note: This procedure has you select a directory in which to place installation files. You may want to create this directory before you start this procedure. Also, you need to authenticate with administrative credentials to the Windows Domain or Workgroup that contain the computers.

Deploying client software to computers that run firewalls, and that run Windows XP, Windows Vista, or Windows Server 2008 have special requirements. Firewalls must permit remote deployment over TCP ports 139 and 445. Also, the computers that are in workgroups and that run Windows XP must disable simple file sharing. Windows Vista and Windows Server 2008 have additional requirements.

You can also use the Find Unmanaged Computers utility that lets you discover the client computers that do not run client software and then install the client software on those computers.

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

To configure client software

- 1 Start the Migration and Deployment Wizard by doing one of the following:
 - On the Windows Start menu, click **Start > Programs > Symantec Endpoint Protection Manager > Migration and Deployment Wizard**.
The path may be different depending on the version of Windows you use.
 - On the last panel of the Management Server Configuration Wizard, click **Yes**, and then click **Finish**.
See “Installing and configuring the Symantec Endpoint Protection Manager with an embedded database” on page 20.
- 2 In the Welcome to the Migration and Deployment Wizard panel, click **Next**.
- 3 In the What would you like to do panel, check **Deploy the client** (Symantec Endpoint Protection only), and then click **Next**.
- 4 In the next panel, check **Specify the name of a new group that you wish to deploy clients to**, type a group name in the box, and then click **Next**.
After you have deployed client software and logged on to the console, you can locate this group in the console.
- 5 In the next panel, uncheck any types of protection that you do not want to install (Symantec Endpoint Protection only), and then click **Next**.
- 6 In the next panel, check the installation options that you want for packages, files, and user interaction.
- 7 Click **Browse**, locate and select a directory in which to place the installation file(s), and then click **Open**.

8 Click **Next**.

9 In the next panel, check **Yes**, and then click **Finish**.

It can take several minutes to create and export the installation package for your group before the Push Deployment Wizard appears.

To deploy the client software with the Push Deployment Wizard

1 In the Push Deployment Wizard, under Available computers, expand the trees and select the computers on which to install the client software, and then click **Add >**.

2 In the Remote Client Authentication dialog box, type the user name and password, and then click **OK**.

The user name and password must be able to authenticate to the Windows Domain or Workgroup that contains the computers.

3 When you have selected all of the computers and they appear in the right pane, click **Finish**.

Logging on to the Symantec Endpoint Protection Manager Console

The Symantec Endpoint Protection Manager Console lets you perform administrative tasks such as managing clients and policies.

To log on to the Symantec Endpoint Protection Manager Console

1 Click **Start > Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Console**.

2 In the Symantec Endpoint Protection Manager logon prompt, in the User name box, type **admin**.

3 In the Password box, type the admin password that you created during installation, and then click **Log On**.

Adding a group

You can add groups after you define the group structure for your organization.

Group descriptions may be up to 1024 characters long. Group names and descriptions may contain any character except the following characters: [" / \ * ? < > | :].

Note: You cannot add groups to the Default Group.

To add a group

- 1 In the console, click **Clients**.
- 2 Under View Clients, select the group to which you want to add a new subgroup.
- 3 On the Clients tab, under Tasks, click **Add Group**.
- 4 In the Add Group for *group name* dialog box, type the group name and a description.
- 5 Click **OK**.

About policies

Symantec Endpoint Protection Manager lets you configure and assign policies to groups or locations in groups. All client computers that are in the groups and locations receive the permissions and features that are specified in the policies. For example, if a LiveUpdate Settings Policy specifies to run LiveUpdate daily at 10:00 P.M., all clients that receive that policy run LiveUpdate daily.

For Symantec Endpoint Protection, multiple policies exist. Policies exist for LiveUpdate, Antivirus and Antispyware Protection, Centralized Exceptions, and so forth.

Note: For legacy Symantec AntiVirus and Symantec Client Security users, the settings that applied to groups, management servers, and clients now are contained in policies.

See “About LiveUpdate policies for client updates” on page 27.

See “Configuring and testing Symantec Endpoint Protection” on page 29.

Configuring LiveUpdate for site updates

You should configure the frequency that the Symantec Endpoint Protection Manager checks for and downloads new updates to the site. You also configure client updates with LiveUpdate Content Policies and LiveUpdate Settings Policies. You should make sure to download all types that you want clients to receive.

Symantec Endpoint Protection Manager for Symantec Network Access Control only supports product updates.

To configure LiveUpdate for the site

- 1 In the console left pane, click **Admin**.
- 2 In the lower-left pane, click **Servers**.
- 3 In the upper-left pane, right-click **Local Site**, and then click **Edit Properties**.
- 4 On the LiveUpdate tab, under Download Schedule, check the Frequency options with which to download the latest definitions.
- 5 For details about setting other options in this dialog box, click **Help**.
- 6 When you finish setting the site's LiveUpdate properties, click **OK**.

About LiveUpdate policies for client updates

You configure LiveUpdate for clients by using two types of LiveUpdate Policies. A LiveUpdate Settings Policy specifies the frequency that clients run LiveUpdate to check for product or content updates. A LiveUpdate Content Policy specifies the type of content that clients can receive when they run LiveUpdate (Symantec Endpoint Protection only).

When you create a group with the Migration and Deployment Wizard, the group receives a default LiveUpdate Settings Policy and a default LiveUpdate Content Policy. For the group to use either policy, you must assign the policy to the group. For example, you can create a LiveUpdate Settings Policy that is called MyLiveUpdate Policy and assign it to a group that uses a default policy. The new MyLiveUpdate policy then takes the place of the default policy. Other groups can also share the new policy that you create.

Configuring a LiveUpdate Settings Policy

By default, clients receive a LiveUpdate Settings Policy. You can either create a new policy and replace the default policy, or edit the default policy.

To configure a LiveUpdate Settings Policy

- 1 On the console, click **Policies**.
- 2 In the View Policies pane, click **LiveUpdate**.
- 3 In the lower-left Tasks pane, click **Add a LiveUpdate Settings Policy**.
- 4 In the Overview pane, in the Policy name box, type a name for the policy.
- 5 Under LiveUpdate policy, click **Schedule**.
- 6 In the Schedule pane, accept or change the scheduling options.
- 7 Under LiveUpdate Policy, click **Advanced Settings**.

- 8 Decide whether to keep or change the default settings.
For details about the settings, click **Help**.
Generally, you do not want users to modify update settings. However, you may want to let them manually launch a LiveUpdate session if you do not support hundreds or thousands of clients.
- 9 When you have configured your policy, click **OK**.
- 10 In the Assign Policy dialog box, click **Yes**.
- 11 In the Assign LiveUpdate Policy dialog box, check the groups and locations to which to apply the policy, and then click **Assign**.
If you cannot select a nested group, that group inherits policies from its parent group, as set on the Policies tab of the Clients page.
- 12 In the Assign LiveUpdate Policy dialog box, click **Yes**.

Configuring a LiveUpdate Content Policy

By default, all clients in a group receive the latest versions of all content updates. However, clients receive only the updates that the management server downloads. A LiveUpdate Content Policy can be configured to get updates from a management server. If so, the management server must be configured to allow all updates, or the clients receives only the updates the server downloads. You can configure the updates that the server downloads from the Admin pane of the console.

Note: LiveUpdate Content Policies are not available for Symantec Network Access Control clients.

To configure a LiveUpdate Content Policy

- 1 In the console, click **Policies**.
- 2 In the View Policies pane, click **LiveUpdate**.
- 3 In the LiveUpdate Policies pane, click the **LiveUpdate Content** tab.
- 4 In the lower-left Tasks pane, click **Add a LiveUpdate Content Policy**.
- 5 In the Overview pane, in the Policy name box, type a name for the policy.
- 6 If you configure Symantec Endpoint Protection, in the LiveUpdate Content pane, click **Security Definitions**.
- 7 In the Security Definitions pane, check the updates to download and install, and uncheck the updates to disallow.
- 8 In the LiveUpdate Content Policy window, click **OK**.

- 9 In the Assign Policy dialog box, click **Yes**.
- 10 In the Assign LiveUpdate Content Policy dialog box, check one or more groups to which to apply this policy, and then click **Assign**.
If you cannot select a nested group, that group inherits policies from its parent group, as set on the Policies tab of the Clients page.
- 11 In the Assign LiveUpdate Policy dialog box, click **Yes**.

Configuring and testing Symantec Endpoint Protection

After you configure and install a LiveUpdate Policy, you should create and apply an Antivirus and Antispyware Policy.

Note: This section assumes that you purchased and installed Symantec Endpoint Protection.

Configuring a default Antivirus and Antispyware Policy

You should configure an Antivirus and Antispyware Policy for your group. In this procedure, you edit the default policy that is currently only applied to the group. You can, however, create a new policy and apply it to your group.

To configure a default Antivirus and Antispyware Policy

- 1 On the console, in the left pane, click **Clients**.
- 2 Under View Clients, select a group, and click the **Policies** tab.
- 3 On the Policies tab, under Location-specific Policies and Settings, across from Antivirus and Antispyware Policy [shared], click **Tasks > Convert to Non-shared Policy**.
- 4 In the Antivirus and Antispyware Policy pane, click **File System Auto-Protect**.
- 5 On the Scan Details tab, verify that **Enable File System Auto-Protect** is checked, and that the lock icon is in the unlocked mode (for testing).
Generally, you want this setting locked, but for initial testing purposes, leave it unlocked. Locking a setting prevents users from changing a setting.
- 6 On the Actions tab, under Detection, click **Non-macro virus**.

- 7 Under Actions for: Non-macro virus, inspect the default sequence of actions that occur when a non-macro virus is detected.
The first action is to try to clean the virus. If it is not possible to clean, the virus is quarantined.
- 8 On the Notifications tab, inspect the message that appears on client computers when a virus or security risk is detected.
You can change this message later if necessary.
- 9 In the left pane, click **Administrator-defined scans**.
- 10 On the Scans tab, under Name, click **Weekly Scheduled Scan**, and then click **Edit**.
- 11 Become familiar with the options on the different tabs and change them if necessary.
Full scans are always recommended initially. After full scans are run, Active scans and Auto-Protect are effective to secure client computers.
- 12 When you understand the scan options, click **OK**.
- 13 In the left pane, click **Quarantine** and then click **Cleanup**.
- 14 On the Cleanup tab, review the settings for purging repaired and quarantined files.
Become familiar with these settings if you want to change them in the future.
- 15 Click **OK**.

Testing antivirus capabilities

You should experiment with antivirus detection in a controlled test environment to become familiar with alerts and log entries. Before you test antivirus detection, download the latest antivirus test file Eicar.com onto transportable media such as a memory stick. You can download Eicar.com at the following URL:

<http://www.eicar.org>

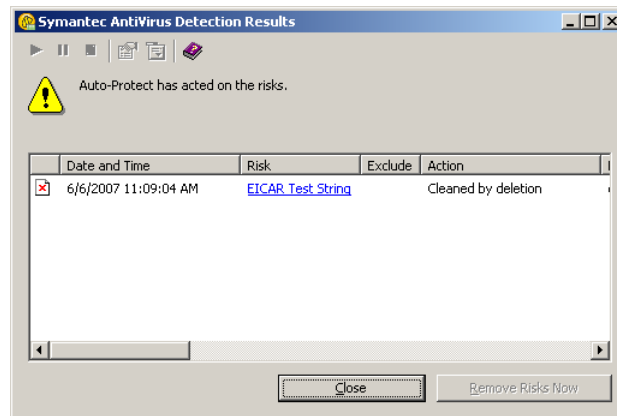
Testing Auto-Protect

Auto-Protect is the Symantec real-time process that inspects every file that executes or is user-accessed to see if it is a virus or security risk. Auto-Protect determines whether files are viruses or security risks by using the definitions that you download from Symantec. You can see how Auto-Protect works by using a benign virus called Eicar. Several versions are available at the following URL:

<http://www.eicar.org>

To test Auto-Protect

- 1 On a client computer, in the lower-right corner, right-click the Symantec Endpoint Protection shield, and click **Disable Symantec Endpoint Protection**.
- 2 If you have not downloaded eicar.com, go to <http://www.eicar.org>, and then locate and download eicar.com to the client computer.
- 3 In the lower-right corner, right-click the Symantec Endpoint Protection shield, and click **Enable Symantec Endpoint Protection**.
- 4 Double-click **eicar.com**.



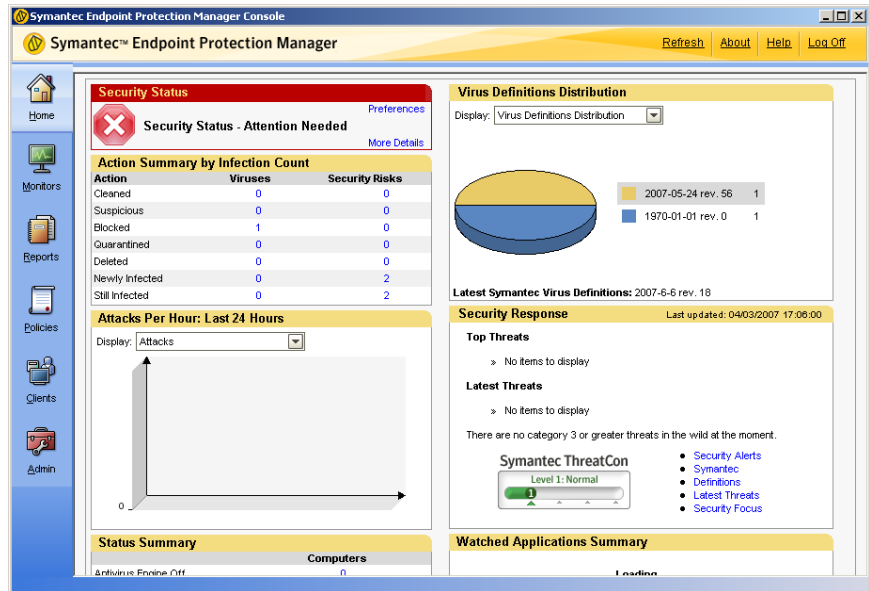
- 5 Read and become familiar with the details in the message prompt(s).

Managing the detected threat

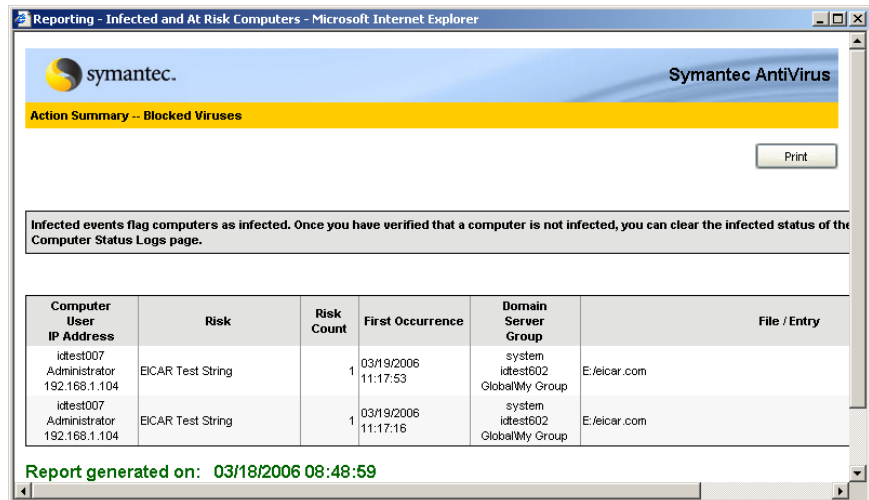
After Symantec Endpoint Protection detects and isolates eicar.com, it sends the information to Symantec Endpoint Protection Manager. You can then see that the activity that occurred from the Home page in Symantec Endpoint Protection Manager Console. This task is a primary task that you perform in a production environment. When clients detect real threats, you first display details about the threat. You then decide if Auto-Protect mitigated the threat and then clear the status.

To manage the detected threat

- 1 In the console, click **Home**.

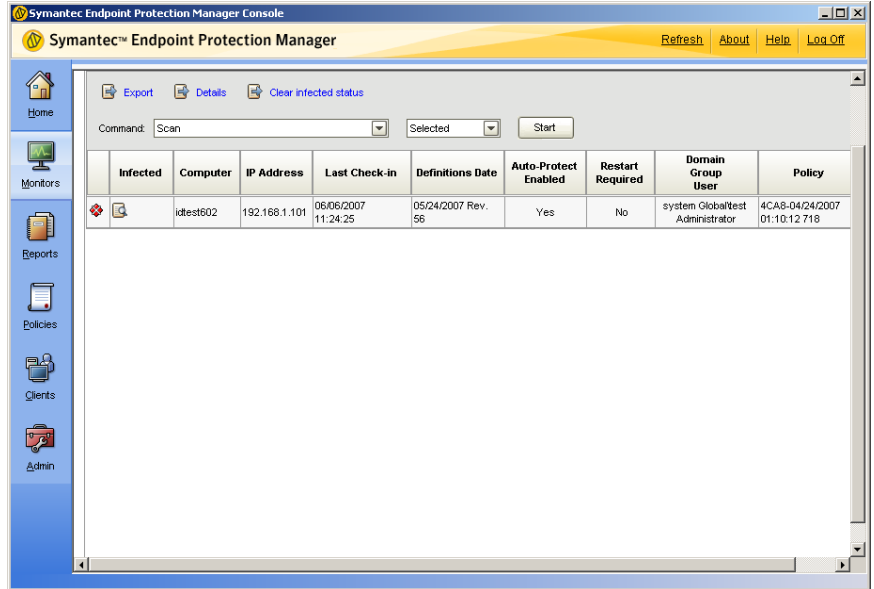


- 2 In the Viruses column for the Blocked row, click the number.



- 3 In the Reporting - Infected and At Risk Computers window, become familiar with the reported information, and then close the window.
- 4 Click **Monitors**.

- 5 On the Logs tab, in the Log type drop-down, click **Computer Status**, and then click **View Log**.



- 6 To display information about the infection, click **Details**.
- 7 To clear the Infected Status, click **Clear infected status**.

Configuring the Security Status icon

The Home page displays the security status of your client computers. The two possible statuses are Good and Attention Needed. You can control when the status is Good and Attention Needed by setting security status threshold preferences.

To configure the Security Status icon

- 1 In the console, click **Home**.
- 2 Under Security Status, click **More Details**.
- 3 In the Security Status Details window, review the features that trigger the Good and Attention Needed status.
- 4 Close the window.
- 5 Under Security Status, click **Preferences**.
- 6 In the Preferences dialog box, on the Security Status tab, review the security status triggers and thresholds that you can set.

All thresholds default to 10 percent.

- 7 For security status details, click **Help**.
To trigger the Attention Needed status, disable Symantec Endpoint Protection on one of your test clients.
- 8 Click **OK**.
- 9 To review the security status of your managed clients at any time, on the Home page, click the **Status** icon.

Where to get more information about Symantec Endpoint Protection and Symantec Network Access Control

Sources of information include the following:

- *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control*
- *Client Guide for Symantec Endpoint Protection and Symantec Network Access Control*
- *LiveUpdate Administration Guide* (Symantec Endpoint Protection only)
- *Symantec Central Quarantine Administration Guide* (Symantec Endpoint Protection only)
- *Solutions Guide for Symantec™ Endpoint Protection and Symantec Network Access Control*
- *Symantec Endpoint Protection 11.0 Best Practices White Paper for Microsoft Small Business Server 2003* (Symantec Endpoint Protection only)
- *Readme* files, located in the root folder of the installation CD
- Online Help that contains all of the content that is in the guides and more

The primary documentation is available in the Documentation folder on the product discs. Some individual component folders contain component-specific documentation. Updates to the documentation are available from the Symantec Technical Support Web site.

Where to get more information about Symantec Endpoint Protection and Symantec Network Access Control

Table 1-7 Symantec Web sites

Types of information	Web address
Public Knowledge Base Releases and updates Manuals and documentation updates Contact options	http://www.symantec.com/techsupp/enterprise/
Release notes and additional post-release information	http://www.symantec.com/business/support/overview.jsp?pid=54619
Virus and other threat information and updates	http://securityresponse.symantec.com
Product news and updates	http://enterprisesecurity.symantec.com
Symantec Endpoint Protection forums	https://forums.symantec.com/syment/board?board.id=endpoint_protection11

