Implementation Guide for Symantec™ Endpoint Protection Small Business Edition

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 12.00.00.00.00

Legal Notice

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

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	supportsolutions@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.

Contents

Chapter 1

Introducing Symantec Endpoint Protection Small Business Edition

This chapter includes the following topics:

About Symantec Endpoint Protection Small Business Edition

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

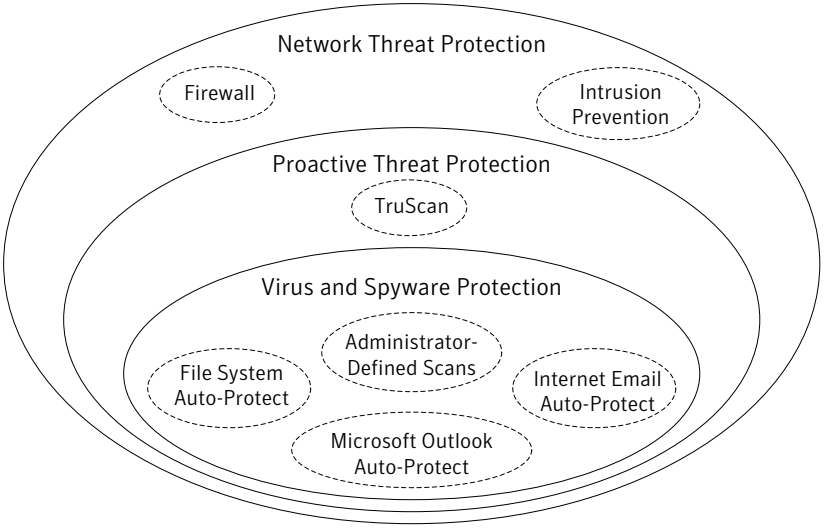
Symantec Endpoint Protection Small Business Edition is a client-server solution that protects the client computers in your network. Providing low maintenance and high power, Symantec Endpoint Protection Small Business Edition

communicates over your network to automatically safeguard computers against viruses and security threats.

About the types of protection

The Symantec Endpoint Protection Small Business Edition client enforces virus and other protection technologies on the client computers using three layers of essential protection.

Figure 1-1 Protection layers



The Virus and Spyware Protection layer combats a wide range of threats that include spyware, worms, Trojan horses, rootkits, and adware. Administrator-defined scans inspect all parts of a computer, including the boot sector and floppy drives. File System Auto-Protect continuously inspects all computer files for viruses and security risks. Internet Email Auto-Protect scans the email messages that use the POP3 or SMTP communications protocol over the Secure Sockets Layer (SSL). Microsoft Outlook Auto-Protect scans Outlook email messages.

The Proactive Threat Protection layer uses a unique Symantec technology called TruScan proactive threat scan. TruScan proactive threat scan protects against unseen, or zero-day, threats by analyzing suspicious behavior from an application or process.

The Network Threat Protection layer comprises firewall and Intrusion Prevention protection. The rules-based firewall prevents unauthorized users from accessing

your computers and networks. Intrusion Prevention automatically detects and blocks network attacks.

Single console management

You manage the protection technologies in Symantec Endpoint Protection Small Business Edition from a single console. Using a graphical user interface, you deploy the protection technologies to your computers and monitor the endpoint status—all from one console. You can log on to the console locally, or you can log on remotely. Administrators can set up users with portable computers to manage protection directly from the Symantec Endpoint Protection Small Business Edition client.

Administrators configure clients to get virus definitions and product updates by using one of the following methods:

- Get virus definitions and product updates from Symantec Protection Center.
- Get virus definitions and product updates from the Symantec LiveUpdate server.

How you are protected out-of-the-box

When you install Symantec Endpoint Protection Small Business Edition, all protection technologies are installed, but not all the technologies are enabled by default. Symantec Endpoint Protection Small Business Edition includes Symantec security policies that have default settings. The policies are configured for out-of-the-box protection for small business customers. The policies balance the need for protection with performance.

See "About the client installation settings" on page 47.

The Symantec security policies define the protection technologies settings that are used to protect your computers from known and unknown threats. A default policy is provided for each type of protection. While the default policies provide appropriate settings for most small businesses, you may want to adjust settings over time based on your company needs. You can review the default settings for each policy protection type.

See "About the security policies" on page 82.

LiveUpdate provides continuous product support by downloading virus definitions and product updates. Client computers get content updates from Symantec Protection Center. Or, you can allow client computers to get content updates directly from the Symantec LiveUpdate server. You can adjust the default schedules that the server and the client computers use to get content updates.

See "How clients receive content updates" on page 90.

Key features of Symantec Endpoint Protection Small Business Edition

Table 1-1 lists the key features of Symantec Endpoint Protection Small Business Edition.

Table 1-1 Product key features

Feature	Description
Enterprise-level protection	The product includes the following features: ■ Detect and repair the effects of known viruses, worms, Trojan horses, spyware, adware, and rootkits. ■ Analyze processes for behavior anomalies to detect known and unknown viruses and security risks. ■ Prevent unauthorized users from accessing the computers and networks that connect to the Internet. ■ Automatically detect and block network attacks.
Management	The following features are included: ■ Out-of-the-box configuration for small business. ■ Single console provides a view of the entire client deployment. ■ Symantec Protection Center coordinates console and client communication and event logging. ■ Administrator accounts provide access to the console. ■ LiveUpdate downloads the latest virus definitions and product updates.
Migration	The following features are included: ■ Group and policy settings migration from Symantec legacy virus protection software. ■ Client computer upgrade using the Client Installation Wizard.
Client enforcement	The following features are included: ■ Client computer scanning for viruses and security threats. ■ Cleaning, deleting, and quarantining of infected files.

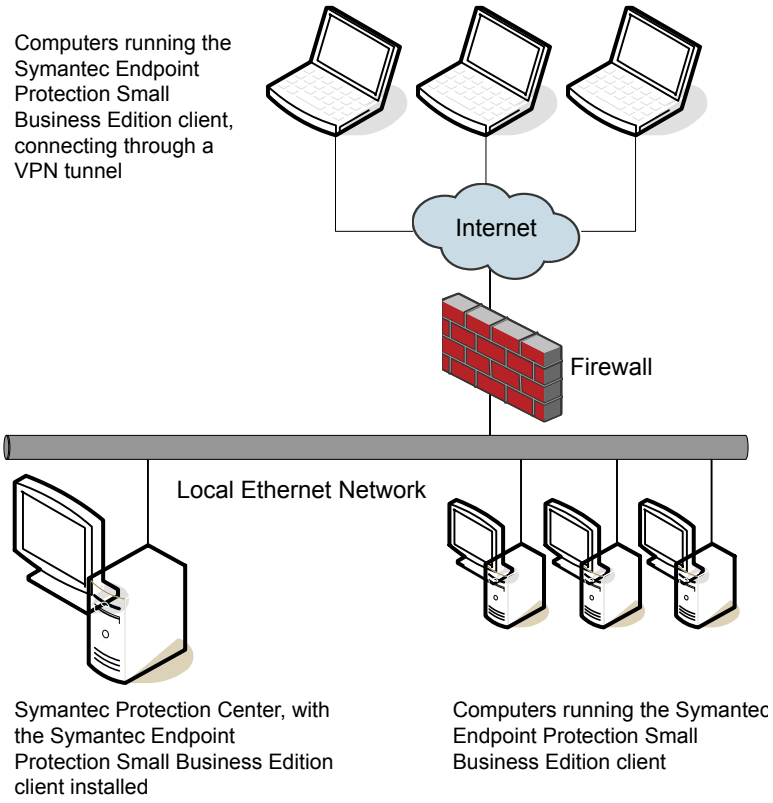
Components of Symantec Endpoint Protection Small Business Edition

Table 1-2 lists the Symantec Endpoint Protection Small Business Edition components.

Table 1-2 Product components

Component	Description
Symantec Protection Center	Symantec Protection Center centrally manages the client computers that connect to your company's network. Symantec Protection Center comprises the following software: ■ The console software coordinates and manages security policies and client computers. ■ The server software provides secure communication to and from the client computers and the console.
Database	A database stores security policies, events, and product licenses. The database is installed on the computer that hosts Symantec Protection Center.
Symantec Endpoint Protection Small Business Edition client	The Symantec Endpoint Protection Small Business Edition client enforces virus and other protection technologies on the client computers. It runs on the servers, desktops, and portable computers that you want to protect.

Figure 1-2 Symantec Endpoint Protection Small Business Edition components



Where to get more information about Symantec Endpoint Protection Small Business Edition

Symantec Endpoint Protection Small Business Edition includes the following sources of information:

- *Getting Started Guide for Symantec Endpoint Protection Small Business Edition*
- *Implementation Guide for Symantec Endpoint Protection Small Business Edition*
- *Client Guide for Symantec Endpoint Protection Small Business Edition*
- *Remote Installation Troubleshooting*
  This file includes background information on the Push Deployment Wizard. The Push Deployment Wizard helps you deploy the client software on computers remotely from a computer that does not run Symantec Protection

Center. You can find the tool in the Tools\PushDeploymentWizard folder of the product disc.

- *Symantec Client Firewall Policy Migration Guide*
  This guide includes information on how to convert policies from Symantec Client Firewall Administrator to Symantec Protection Center.
- *Readme for Symantec Endpoint Protection Small Business Edition*
- Online Help for Symantec Protection Center
- Online Help for the Symantec Endpoint Protection Small Business Edition client

The user documentation might be updated between product releases.

You can locate the latest user documentation at the Symantec Technical Support Web site.

Technical Support resources

Table 1-3 lists the Symantec Web sites where you can find more information .

Table 1-3 Symantec Web sites

Types of information	Web address
Symantec Endpoint Protection Small Business Edition trialware	http://www.symantec.com/business/products/downloads/
Public Knowledge Base Releases Manuals and documentation updates Contact options Release Notes and additional post-release information	http://www.symantec.com/business/support/overview.jsp?pid=55357
Virus and other threat information and updates	http://securityresponse.symantec.com
Product news and updates	http://enterprisesecurity.symantec.com
Symantec Endpoint Protection Small Business Edition forums	http://www.symantec.com/community
Free online technical training	http://www.symantec.com/education/endpointsecurity

Chapter 2

Planning the installation

This chapter includes the following topics:

Planning the installation

Table 2-1 summarizes the installation steps for Symantec Endpoint Protection Small Business Edition.

Table 2-1 Installation planning

Step	Action	Description
Step 1	Plan network architecture	Identify the computers on which you want to install Symantec Endpoint Protection Small Business Edition. See "Network architecture considerations" on page 23.
Step 2	Review product license requirements	Purchase a license within 30 days of product installation. See "Product license requirements" on page 25.

Table 2-1 Installation planning *(continued)*

Step	Action	Description
Step 3	Review system requirements	Make sure your computers comply with the minimum system requirements. See "System requirements" on page 25.
Step 4	Prepare computers for installation	Uninstall other virus protection software from your computers. See "Preparing your computers for installation" on page 28.
Step 5	Identify installation settings	Identify the user names, passwords, email addresses, and other installation settings. Have the information on hand during the installation. See "About the Symantec Protection Center installation settings" on page 33. See "About the client installation settings" on page 47.
Step 6	Install server	Install Symantec Protection Center. See "Installing Symantec Protection Center" on page 31.
Step 7	Migrate Symantec legacy virus protection software	Optionally migrate policy and group settings from your Symantec legacy virus protection software. See "About migrating to Symantec Endpoint Protection Small Business Edition" on page 55.
Step 8	Prepare computers for client installation	Prepare for client installation as follows: ■ Identify the methods to use to deploy the client software to your computers. ■ Uninstall third-party virus protection software from your computers. ■ Modify or disable the firewall settings on your computers. ■ Prepare your computers for remote client deployment. ■ Set up the console computer groups to match your organizational structure. See "Preparing for client installation" on page 41.
Step 9	Install clients	Install the Symantec Endpoint Protection Small Business Edition client on your unprotected computers. Symantec recommends that you also install the client on the computer that hosts Symantec Protection Center. See "Installing the Symantec Endpoint Protection Small Business Edition client" on page 45.
Step 10	Identify post-installation tasks	Identify the tasks that you want to perform after you install Symantec Endpoint Protection Small Business Edition. See "What to do after you install Symantec Protection Center" on page 37.

Network architecture considerations

You can install Symantec Endpoint Protection Small Business Edition for testing purposes without considering your company network architecture. You can install Symantec Protection Center with a few clients, and become familiar with the features and functions.

When you are ready to install the production clients, you should plan your deployment based on your organizational structure and computing needs.

You should consider the following elements when you plan your deployment:

- Symantec Protection Center
  Administrators use Symantec Protection Center to manage security policies and client computers. You may want to consider the security and availability of the computer on which Symantec Protection Center is installed.
- Remote console
  Administrators can use a remote computer that runs the console software to access Symantec Protection Center. Administrators may use a remote computer when they are away from the office. You should ensure that remote computers meet the remote console requirements.
- Local and remote computers
  Remote computers may have slower network connections. You may want to use a different installation method than the one you use to install to local computers.
- Portable computers such as notebook computers
  Portable computers may not connect to the network on a regular schedule. You may want to have portable computers get updates from the LiveUpdate server rather than Symantec Protection Center.
- Computers that are located in secure areas
  Computers that are located in secure areas may need different security settings from the computers that are not located in secure areas.

You identify the computers on which you plan to install the client. Symantec recommends that you install the client software on all unprotected computers, including the computer that runs Symantec Protection Center.

You decide how you want to manage the computers. In most cases, you manage the computers from the console. You might want to manually manage the portable computers that connect to the company network intermittently, such as mobile devices like notebook computers. Computers that never connect to the company network must be managed manually.

You organize the computers with similar security needs into groups. For example, you might organize the computers in the Payroll department into the Payroll group. The group structure that you define most likely matches the structure of your organization.

You create the groups by using Symantec Protection Center. Adjust the security policy settings for the groups that require additional restrictions.

You assign the computers to the groups. You can assign computers to groups during client installation. You can also assign computers to groups from the console after client installation.

Guidelines for managing portable computers

Symantec Endpoint Protection Small Business Edition protects your portable computers from viruses and security threats. A portable computer is a laptop computer or notebook computer that moves physically from one location to another. A portable computer might connect to your network intermittently or not at all. A portable computer might connect to your network through a virtual private network or a wireless network.

Consider the following best practices for managing portable computers:

- Install the portable computers as managed computers.
  Administering managed computers is easy, because you access the managed computers directly from Symantec Protection Center.
  If your company uses any portable computers that never connect to the network, install the portable computers as unmanaged computers. Unmanaged computers do not communicate with Symantec Protection Center.
- Create a group for the managed portable computers.
  Placing the managed portable computers in one group lets you manage the computers as a single unit.
- Strengthen the protection technologies for remote users.

About trialware

Trialware is a trial version of Symantec Endpoint Protection Small Business Edition. You can use trialware to learn about the product firsthand. You can use trialware to evaluate and test the product.

Trialware includes the following trial software:

- Symantec Protection Center
- Symantec Endpoint Protection Small Business Edition client

- Database for storing security policies and events
- Access to LiveUpdate content

You may visit the following Trialware Web site to download trialware for Symantec Endpoint Protection Small Business Edition:

http://www.symantec.com/business/products/downloads/

See "Product license requirements" on page 25.

Product license requirements

Symantec Endpoint Protection Small Business Edition requires that you purchase a product license.

Table 2-2 Product license requirements

Product	Description
Fully licensed installation	The license requirements are as follows: ■ You must purchase a license for each client computer that you deploy. ■ You must register the product serial number. ■ You must import the license file into the Symantec Protection Center console.
Symantec legacy virus protection software	Symantec Endpoint Protection Small Business Edition accepts the license file from your Symantec legacy virus protection software. You must purchase a new license when the legacy license expires.
Trialware	A 30-day trial license is included with Symantec Endpoint Protection Small Business Edition. You must purchase a license when the trial license expires.

System requirements

Symantec Endpoint Protection Small Business Edition requires specific operating systems and hardware. All the computers on which you install the product should meet or exceed the recommended system requirements.

The Symantec Protection Center system requirements are as follows:

- 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 Intel Itanium IA-64 is not supported.
- Operating systems: Windows 2000 Server, Windows XP (32-bit, 64-bit), Windows Server 2003 (32-bit, 64-bit), Windows Server 2008 (32-bit, 64-bit), Windows Small Business Server 2008 (64-bit), or Windows Essential Business Server 2008 (64-bit)
  Windows Vista (32-bit, 64-bit) is not officially supported.
- RAM memory: 1 GB of RAM minimum (2 GB of RAM recommended)
- Hard disk: 4 GB or more free space

The client system requirements are as follows:

- 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 Intel Itanium IA-64 is not supported.
- Operating systems: Windows 2000 Professional/Server, Windows XP (32-bit, 64-bit), Windows XP Embedded , Windows Vista (32-bit, 64-bit), Windows Server 2003 (32-bit, 64-bit), Windows Server 2008 (32-bit, 64-bit), Windows Small Business Server 2008 (64-bit), or Windows Essential Business Server 2008 (64-bit)
- RAM memory: 256 MB of RAM minimum (1 GB of RAM recommended)
- Hard disk: 700 MB or more free space
- Browser: Internet Explorer 6 or later
  The Remote Push Installation client deployment method does not verify that Internet Explorer 6.0 or later is installed on computers. If the computers do not have the correct version of Internet Explorer, the installation fails without warning.

Internationalization requirements

Certain restrictions apply when you install Symantec Protection Center in a non-English or mixed-language environment.

Table 2-3 Internationalization requirements

Component	Requirements
Computer names, server names, and work group names	Non-English characters are supported with the following limitations: ■ Network audit may not work for a host or user that uses a double-byte character set or a high-ASCII character set. ■ Double-byte character set names or high-ASCII character set names may not appear properly on the Symantec Protection Center console or on the client user interface. ■ A long double-byte or high-ASCII character set host name cannot be longer than what NetBIOS allows. If the host name is longer than what NetBIOS allows, the Home, Monitors, and Reports pages do not appear on the Symantec Protection Center console.
English characters	English characters are required in the following situations: ■ Deploy a client package to a remote computer. ■ Define the server data folder in the Server Configuration Wizard. ■ Define the installation path for Symantec Protection Center. ■ Define the credentials when you deploy the client to a remote computer. ■ Define a group name. You can create a client package for a group name that contains non-English characters. You might not be able to deploy the client package using the Push Deployment Wizard when the group name contains non-English characters. ■ Push non-English characters to the client computers. Some non-English characters that are generated on the server side may not appear properly on the client user interface. For example, a double-byte character set location name does not appear properly on non-double-byte character set named client computers.

VMware support

Symantec software is supported on VMware.

Table 2-4 VMware support

Symantec software	VMware support
Symantec Protection Center and database	Symantec Protection Center is supported on the following VMware versions: ■ VMware WS 5.0 (workstation) or later ■ VMware GSX 3.2 (enterprise) or later ■ VMware ESX 2.5 (workstation) or later Symantec Protection Center is supported on the following guest VMware operating systems: ■ Windows 2000 Professional/Server/Advanced Server SP 3 or later ■ Windows Server 2003 Editions ■ Windows Server 2003 x64 Editions ■ Windows XP Home Edition/Professional ■ Windows XP Professional x64 Edition
Client	The client is supported on the following VMware versions: ■ VMware WS 5.0 (workstation) or later ■ VMware GSX 3.2 (enterprise) or later ■ VMware ESX 2.5 (workstation) or later The client is supported on the following guest VMware operating systems: ■ Windows 2000 Professional/Server/Advanced Server ■ Windows Server 2003 Editions ■ Windows Server 2003 x64 Editions ■ XP Professional/Home Edition Windows ■ XP Professional x64 Edition

About Microsoft Virtual Server support

Symantec software is supported on Microsoft Virtual Server 2005.

Preparing your computers for installation

You must prepare your computers for installation before you install Symantec Endpoint Protection Small Business Edition.

To prepare your computers for installation

1 Uninstall third-party virus protection software.

Symantec does not recommend that you run two virus protection programs on the same computer. The programs can affect the performance and effectiveness of Symantec Endpoint Protection Small Business Edition.

Follow your company's software removal procedure to uninstall your third-party virus protection programs. For example, you can use the Windows Add or Remove Programs tool to uninstall the programs.

See your third-party documentation for information about uninstalling the virus protection programs.

See your Windows documentation for information about the Add or Remove Programs tool.

2 Uninstall your Symantec legacy virus protection software if you do not plan to migrate the settings.

See "About migrating to Symantec Endpoint Protection Small Business Edition" on page 55.

See your Symantec documentation for information on uninstalling the legacy virus protection software.

3 Set administrative rights to your client computers.

To install the client software, you need administrative rights to the computer or to the Windows domain. If you do not want to provide users with administrative rights to their computers, use Remote Push Installation to remotely install the client software. Remote Push Installation requires you to have local administrative rights to the computers.

Client installation upgrades the MSI to version 3.1, which requires administrative rights. If all your computers are upgraded to MSI 3.1, your users only require elevated privileges to install the client.

Chapter 3

Installing Symantec Protection Center

This chapter includes the following topics:

Installing Symantec Protection Center

Table 3-1 lists the steps to install Symantec Protection Center.

Table 3-1 Symantec Protection Center installation summary

Step	Action	Description
Step 1	Identify server computer	Identify the computer on which you plan to install Symantec Protection Center. The computer must run a supported operating system. See "System requirements" on page 25.
Step 2	Prepare computer for installation	Uninstall third-party virus protection software from the computer. See "Preparing your computers for installation" on page 28.

Table 3-1 Symantec Protection Center installation summary *(continued)*

Step	Action	Description
Step 3	Identify installation settings	Installation prompts you to enter values such as the email address that you want to use to receive important notifications. See "About the Symantec Protection Center installation settings" on page 33.
Step 4	Review installation wizards	The installation wizards guide you through the installation of Symantec Endpoint Protection Small Business Edition. See "About the installation wizards" on page 32.
Step 5	Install Symantec Protection Center	You perform several tasks to install the Symantec Protection Center server and console. See "Installing the server and the console" on page 35.

About the installation wizards

The installation wizards guide you through the installation of Symantec Endpoint Protection Small Business Edition.

Table 3-2 Installation wizards

Wizard	Description
Symantec Protection Center Wizard	The Symantec Protection Center Wizard installs Symantec Protection Center. First-time installations always begin with the Symantec Protection Center Wizard. Running the Symantec Protection Center is required.
Management Server Configuration Wizard	The Management Server Configuration Wizard configures Symantec Protection Center. The Management Server Configuration Wizard runs immediately after the Symantec Protection Center Wizard. Running the Management Server Configuration Wizard is required. Symantec Protection Center cannot be used until the Management Server Configuration Wizard completes successfully. After initial product installation, you can run the Management Server Configuration Wizard from the Windows Start menu.

Table 3-2 Installation wizards *(continued)*

Wizard	Description
Migration Wizard	The Migration Wizard migrates the following Symantec legacy virus protection software: ■ Symantec AntiVirus Corporate Edition ■ Symantec Client Security The Migration Wizard runs immediately after the Server Configuration Wizard. Migration is optional; you can quit the Migration Wizard if you do not want to migrate Symantec legacy virus protection software. After initial product installation, you can run the Migration Wizard from the Windows Start menu.
Client Installation Wizard	The Client Installation Wizard installs the client software on unprotected computers. You can run the Client Installation Wizard at any time after you run the Server Installation Wizard and the Server Configuration Wizard. After initial product installation, you can run the Client Installation Wizard from the console.

During initial product installation, the wizards run in the following order:

- Symantec Protection Center Wizard
- Server Configuration Wizard
- Migration Wizard
- Client Installation Wizard

About the Symantec Protection Center installation settings

Server installation prompts you to enter several values.

Table 3-3 Symantec Protection Center installation settings

Setting	Default value	Description
Destination folder	See Description	The directory that is used to install the server software. Required Accept the default directory or click Change to specify another directory. Default directory: C:\Program Files\Symantec\Symantec Protection Center
Company name	none	The name of your company. Optional
User name	admin	The administrator account user name that you use to log on to the console. You can change the default user name after initial product installation. See "Editing an administrator account" on page 145.
Password	none	The password for the administrator account. Required Type a password of your choice, and then type it again to confirm. You can change the password after initial product installation. See "Resetting a forgotten password" on page 64.
Email address	none	The email address that you want to use to receive important reports and notifications. Notifications about events such as virus detections are sent to the email address that you provide. Make sure you specify a valid email address that you regularly use so that you receive the notifications. Required
Server name	host name of the local computer	The address of your SMTP email server. Symantec Protection Center uses the email server to send alerts and notifications to your email address. Required If you do not know the address of your SMTP server, contact your administrator or ISP. In most cases, you accept the default.

Table 3-3 Symantec Protection Center installation settings *(continued)*

Setting	Default value	Description
Port number	25	The email server port number. Symantec Protection Center uses the port number to communicate with your email server. Required If you do not know the port number, contact your administrator or ISP. In most cases, you accept the default.

Table 3-4 lists the server settings that are preset during installation. You can change the settings after the initial product installation by running the Server Configuration Wizard.

Table 3-4 Preset server installation settings

Setting	Default value	Description
Server name	host name of the local computer	The name of the computer that hosts Symantec Protection Center.
Server port	8443	The HTTPS port that the Symantec Protection Center console uses.
Admin GUI Access port	9090	The HTTP port that remote console connections use.
Client communications port	8014	The port that the client computers use to communicate with the computer that hosts Symantec Protection Center.
Server data folder	See Description	The directory in which Symantec Protection Center places data files, including the database backup files. The installer creates the directory if it does not exist. The default directory is C:\Program Files\Symantec\Symantec Protection Center\data.

Installing the server and the console

You perform several tasks to install the server and the console. A green check mark appears next to a completed task.

To install the server and the console

1. Uninstall third-party virus protection software from the computer.

   See "Preparing your computers for installation" on page 28.

2. 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. See your Windows documentation for information about extracting files from a compressed folder.

   The following options are presented:

Read This First	Select this option to display an overview of the installation.
Install Symantec Endpoint Protection	Select this option to install Symantec Endpoint Protection on the computer.
Install an unmanaged client	Select this option to install the client software on the computer. Unmanaged clients are the portable computers that connect to your company network intermittently or not at all. You manually administer unmanaged clients. Unmanaged clients do not use Symantec Protection Center.
Exit	Select this option to quit the installation.

3. In the Welcome panel, 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**.
7. Configure the server and the console.

   See "Configuring the server" on page 37.

8. Create the database.

   See "Creating the database" on page 37.

9. Optionally migrate your Symantec legacy virus protection installation.

   See "Migrating group settings and policy settings" on page 58.

Configuring the server

To configure the server, you specify the following information:

- The password for the default administrator account.
- The email address that receives important notifications and reports.
- The email server name and port number.

To configure the server

1. In the Administrator Settings panel, specify your company name.
2. In the Administrator Account Creation panel, specify the administrator account password, and then type it again to confirm.
3. In the Administrator Account Creation panel, specify the email address that receives reports and notifications.
4. Click **Next**.
5. In the Email Server Communication Settings panel, accept the default server name and port number or specify other values.
6. In the Email Server Communication Settings panel, click **Send Test Email** to send a test email message to the email address that is associated with the account.
7. Click **Next**.
8. Review the management server port settings.

Creating the database

The database stores policies, events, and licenses.

To create the database

1. In the installation wizard, click **Next** to create the database.
2. Wait while the database is created and initialized.

What to do after you install Symantec Protection Center

Table 3-5 lists the common tasks that you perform after you install Symantec Protection Center.

Table 3-5 Post-installation tasks

Action	Description
Learn about the console	Become familiar with the features and functions of the Symantec Protection Center console. See "About starting the Symantec Protection Center console" on page 61.
Install and migrate clients	Install the client software on your unprotected computers if you have not already done so. See "Installing the Symantec Endpoint Protection Small Business Edition client" on page 45. Optionally migrate your Symantec legacy virus protection software if you have not already done so. See "About migrating to Symantec Endpoint Protection Small Business Edition" on page 55.
Register product serial number, and import license file	Symantec Endpoint Protection Small Business Edition includes a 30-day trial license. You must replace the trial license with a purchased license. See "About managing product licenses" on page 101.
Validate that client computers are online and protected	Run the on-demand scan to check computers for security threats. See "Scanning computers" on page 122. Monitor the protection status on your computers. See "About monitoring endpoint protection" on page 69.
Check the LiveUpdate schedule	Optionally adjust the schedule to check for virus definition and other content updates. See "About managing content updates from LiveUpdate" on page 89.
Check notifications	Notifications alert you about potential security problems. Symantec Protection Center is configured with default notifications. You can adjust the default notifications and create additional notifications. See "About managing notifications" on page 95.
Set up computer groups	Symantec Protection Center is configured with default computer groups. You can create additional groups. See "Creating a group" on page 81.

Table 3-5 Post-installation tasks *(continued)*

Action	Description
Set up administrator accounts	Installation created a default administrator account. You can create additional accounts for administrators and users who need access to the console. See "About administrator accounts" on page 144.

Uninstalling Symantec Protection Center

Uninstalling Symantec Protection Center uninstalls the server, console, and database. You can optionally uninstall the database backup files.

If you plan to reinstall Symantec Protection Center, you should back up the database before you uninstall it.

See "Backing up the database" on page 149.

To uninstall Symantec Protection Center

1. On the server computer, on the Start menu, click **Control Panel > Add or Remove Programs**.
2. In the Add or Remove Programs dialog box, select **Symantec Protection Center**, and then click **Remove**.

Chapter 4

Preparing for client installation

This chapter includes the following topics:

Preparing for client installation

Table 4-1 lists the steps to prepare computers for client installation.

Table 4-1 Client computer preparation

Step	Action	Description
Step 1	Identify client deployment methods	Identify the methods to use to deploy the client software to your computers. See "About deploying clients" on page 48.
Step 2	Remove third-party virus protection software	Uninstall all third-party virus protection software from your computers. See "Preparing your computers for installation" on page 28.
Step 3	Modify or disable firewall settings	Modify or disable the Windows firewall settings. Windows firewalls can interfere with remote client deployment. See "Configuring firewalls for remote deployment" on page 42.
Step 4	Prepare computers for remote deployment	Prepare your computers for remote client deployment. See "Preparing computers for remote deployment" on page 43.

Table 4-1 Client computer preparation *(continued)*

Step	Action	Description
Step 5	Identify computer groups	Identify the computer groups to use during client installation. See "About computer groups" on page 81.

Configuring firewalls for remote deployment

Windows firewalls can interfere with remote client installation and deployment.

Table 4-2 lists the different ways to configure Windows firewall settings, depending on the operating systems to which you install. See your Windows documentation for more information.

Table 4-2 Firewall modifications

Configuration	Description
Permit servers to send and receive traffic to and from TCP ports	Perform the following tasks to install the client software remotely: ■ Permit the server to send traffic from TCP ports 1024-5000 to TCP ports 139 and 145 on the clients. Stateful inspection permits the return traffic automatically. ■ Permit the clients to receive traffic from the server TCP ports 1024-5000 on TCP port 139. You must permit the clients to send traffic from TCP port 139 to TCP ports 1024-5000 on the server. ■ For legacy communications, open UDP port 2967 on all computers.
Disable Windows Firewall in Windows XP, Windows Server 2003, or Windows Server 2008	Windows Firewall can interfere with remote installation and communication between the server and the client computers. If your computers run any of these operating systems, perform one of the following tasks: ■ Disable Windows Firewall on the computers. ■ Leave Windows Firewall enabled, and configure the firewall rules to open ports to permit deployment. **Note:** In Windows XP with SP1, the Windows firewall is called Internet Connection Firewall.

Table 4-2 Firewall modifications *(continued)*

Configuration	Description
Modify the firewalls in Windows Vista or Windows Server 2008	Windows Vista and Windows Server 2008 contain a firewall that is enabled by default. If the firewall is enabled, you might not be able to install or deploy the client software remotely. You can temporarily disable the Windows firewall on the clients before you deploy the client software. If you leave the Windows firewall enabled on the clients, you must configure it to allow file and printer sharing (port 445).

Warning: The firewall in Symantec Endpoint Protection Small Business Edition is disabled by default at initial installation. Leave the Windows firewalls enabled on the clients to ensure firewall protection.

See "Enabling firewall protection" on page 134.

Preparing computers for remote deployment

Table 4-3 lists the actions to prepare your computers for remote deployment of the client software. See your Windows documentation for more information.

Table 4-3 Remote deployment actions

Action	Description
Prepare Windows XP computers that are installed in workgroups	Windows XP computers that are installed in workgroups do not accept remote deployment. To permit remote deployment, disable Simple File Sharing. **Note:** This limitation does not apply to computers that are part of a Windows domain.

Table 4-3 Remote deployment actions *(continued)*

Action	Description
Prepare Windows Vista or Windows Server 2008 computers	Windows User Access Control blocks local administrative accounts from remotely accessing remote administrative shares such as C$ and Admin$. To push the client software to computers, you should use a domain administrative account if the client computer is part of an Active Directory domain. Remote deployment also requires elevated privileges to install. Perform the following tasks: ■ Disable the File Sharing Wizard. ■ Enable network discovery by using the Network and Sharing Center. ■ Enable the built-in administrator account and assign a password to the account. ■ Verify that the account has elevated privileges.
Prepare Windows Server 2003 server for installation using a remote desktop connection	The Symantec Protection Center requires access to the system registry for installation and normal operation. To prepare a computer to install Symantec Endpoint Protection Small Business Edition using a remote desktop connection, perform the following tasks: ■ Configure a server that runs Windows Server 2003 to allow remote control. ■ Connect to the server from a remote computer by using a remote console session, or shadow the console session.

Chapter 5

Installing the Symantec Endpoint Protection Small Business Edition client

This chapter includes the following topics:

Installing the Symantec Endpoint Protection Small Business Edition client

You install the Symantec Endpoint Protection Small Business Edition client after you install Symantec Protection Center.

Table 5-1 Client installation summary

Step	Action	Description
Step 1	Identify client computers	Identify the computers on which you want to install the client software. All the computers must run a supported operating system. See "About managed and unmanaged computers" on page 46.

Table 5-1 Client installation summary *(continued)*

Step	Action	Description
Step 2	Prepare client computers for installation	Uninstall third-party virus protection software from the computers. See "Preparing your computers for installation" on page 28.
Step 3	Identify client installation settings	Installation prompts you to specify the computer group names and the protection types. See "About the client installation settings" on page 47.
Step 4	Deploy client software	Installation prompts you to select one of the following client deployment methods: ■ Email Notification Installation ■ Remote Push Installation ■ Custom Installation See "About deploying clients" on page 48. Symantec recommends that you also install the client on the computer that hosts Symantec Protection Center.

About managed and unmanaged computers

You install client computers as managed or unmanaged computers.

Table 5-2 Client computer types

Type	Description
Managed computer	Managed client computers use Symantec Protection Center. Managed client computers are centrally managed; you administer the computers from the console. Managed client computers connect to your network. You use the console to update the client software, security policies, and virus definitions on the managed client computers. In most cases, you install client computers as managed computers. You can install managed client computers as follows: ■ During initial product installation ■ From the console after installation

Table 5-2 Client computer types *(continued)*

Type	Description
Unmanaged computer	Unmanaged client computers do not use Symantec Protection Center. Unmanaged client computers are self-managed; you or the primary computer users must administer the client computers. In most cases, unmanaged client computers connect to your network intermittently or not at all. You or the primary computer users must update the client software, security policies, and virus definitions on the unmanaged client computers. You install unmanaged client computers directly from the product disc. See "Installing an unmanaged computer" on page 53.

About the client installation settings

Client installation prompts you to specify the computer group names and the protection types.

Table 5-3 Client installation settings

Setting	Default value	Description
Group	Laptops and Desktops	The group that contains the client computers. See "About computer groups" on page 81.

Table 5-3 Client installation settings *(continued)*

Setting	Default value	Description
Protection type	The following default protection technologies are installed: ■ Virus and Spyware Protection ■ Network Threat Protection	The protection technologies that you want to install on the client computers. The protection technologies are as follows: ■ Virus and Spyware Protection Checking this option installs File System Auto-Protect and Proactive Threat Protection. Proactive Threat Protection is disabled on the computers that run supported Windows Server operating systems. ■ Include Email Protection Checking this option installs Microsoft Outlook Auto-Protect and Internet Email Auto-Protect. For performance reasons, Microsoft Outlook Auto-Protect is not installed on supported Microsoft Server operating systems. ■ Network Threat Protection Checking this option installs firewall protection and Intrusion Prevention protection. After installation, you can enable or disable the protection technologies in the security policies. See "About the security policies" on page 82.

About deploying clients

You deploy the Symantec Endpoint Protection Small Business Edition client by using the Client Installation Wizard. The Client Installation Wizard automatically runs during the initial product installation. After the initial product installation, you can run the Client Installation Wizard from the console.

Before you run the Client Installation Wizard, you must identify the client installation settings.

See "About the client installation settings" on page 47.

You deploy the client by using any of the following deployment methods:

- Email Notification Installation
  Users receive an email message that contains a link to download and install the client software. The users must have local administrator rights to their computers. Email notification installation is the recommended deployment method.
  See "Deploying clients by using Email Notification Installation" on page 49.

- Remote Push Installation
  Remote push installation lets you control the client installation. Remote push installation pushes the client software to the computers that you specify. The installation begins automatically.
  See "Deploying clients by using Remote Push Installation" on page 50.
- Custom Installation
  Custom installation creates an executable installation package that you distribute to the client computers. Users run a setup.exe file to install the client software.
  See "Deploying clients by using Custom Installation" on page 51.

Deploying clients by using Email Notification Installation

Email Notification Installation is the recommended method for installing the client software. Email Notification Installation is easy to use. Users receive an email message that contains a link to download and install the client software.

Email Notification Installation performs the following actions:

- Create 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 Protection Center.
- Notify the computer users about the client installation packages.
  An email message is sent to 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. You or the computer users must restart the computers after installation.

You may start the client deployment from the console.

To deploy clients by using Email Notification Installation

1. In the console, click **Home**.
2. On the Home page, in the Common Tasks menu, select Install protection client to computers.
3. In the Client Installation Wizard, select the group to contain the computers.
4. In the Client Installation Wizard, select the protection types, and then click **Next**.

   See "About the client installation settings" on page 47.
5. In the Client Installation Wizard, click **Email Notification Installation**, and then click **Next**.

6 In the Client Installation Wizard, specify the email recipients.

To specify multiple email recipients, type a comma after each email address.

7 In the Client Installation Wizard, accept the default email subject and body or edit the text, and then click **Next**.

8 Click **Finish**.

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

10 You or the computer users must restart the client computers.

See "Restarting client computers" on page 153.

11 Confirm the status of the deployed clients.

See "Viewing client inventory" on page 73.

Deploying clients by using Remote Push Installation

Remote Push Installation lets you control the client installation. Remote Push Installation pushes the client software to the computers that you specify. Remote Push Installation requires knowledge of how to search networks to locate computers.

Remote Push Installation performs the following actions:

- Locate computers on your network.
  Remote Push Installation locates the computers that you specify or the computers that are discovered to be unprotected.
- Push the client software to the computers that you specify.
  To push the client software, you should use a domain administrative account if the client computer is part of an Active Directory domain. Remote Push Installation requires elevated privileges.
  See "Preparing computers for remote deployment" on page 43.
  See "Configuring firewalls for remote deployment" on page 42.
- Install the client software on the computers.
  The installation automatically begins on the computers. You or the computer users must restart the computers after installation.

You may start the client deployment from the console.

To deploy clients by using Remote Push Installation

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

2 On the Home page, in the Common Tasks menu, select Install protection client to computers.

3 In the Client Installation Wizard, select the group to contain the computers.

4 In the Client Installation Wizard, select the protection types, and then click **Next**.

See "About the client installation settings" on page 47.

5 In the Client Installation Wizard, click **Remote Push Installation**, and then click **Next**.

6 In the Client Installation Wizard, locate the computers to receive the client software, and then click **>>** to add the computers to the list.

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**.

Authenticate with the domain or workgroup if prompted.

7 Click **Next**.

You are reminded to install the client on the computer that runs Symantec Protection Center. Installing the client on the computer that runs Symantec Protection Center protects the computer from viruses and security threats. Symantec recommends that you install the client on all your computers.

8 Click **No** to go back and add Symantec Protection Center to the list of computers, or click **Yes** to continue.

9 Click **Send** to push the client software to the selected computers.

10 Wait while the client software is pushed to the selected computers.

11 Click **Finish**.

The installation starts automatically on the client computers. The installation takes several minutes to complete.

12 You or the computer users must restart the client computers.

See "Restarting client computers" on page 153.

13 Confirm the status of the deployed clients.

See "Viewing client inventory" on page 73.

Deploying clients by using Custom Installation

Custom Installation creates the custom packages that can be installed using third-party deployment software or a login script.

Custom Installation performs the following actions:

- Create 32-bit or 64-bit executable installation package.

The installation package can comprise one setup.exe file or a collection of files that include a setup.exe file. Computer users often find one setup.exe file easier to use.

- Save the installation package in the default directory or a directory of your choice.
  The default directory is as follows:
  C:\temp\Symantec\ClientPackages
  You must provide the installation package to the computer users. The users run the setup.exe file to install the client software. You or the computer users must restart the computers after installation.

You may start the client deployment from the console.

To deploy clients by using Custom Installation

1. In the console, click **Home**.
2. On the Home page, in the Common Tasks menu, select Install protection client to computers.
3. In the Client Installation Wizard, select the group to contain the computers.
4. In the Client Installation Wizard, select the protection types, and then click **Next**.

   See "About the client installation settings" on page 47.
5. In the Client Installation Wizard, click **Custom Installation**, and then click **Next**.
6. In the Client Installation Wizard, check **Create a single self-compressed setup.exe** or **Generate all files separately**.
7. In the Client Installation Wizard, in the Export folder box, accept the default directory or specify another directory, and then click **Next**.
8. Review the settings summary, and then click **Next**.
9. Wait while the custom installation package is created.
10. Click **Finish**.
11. Provide the custom installation package to the computer users.

    Save the installation package to a shared network, or email the installation package to the computer users.
12. Confirm that the computer users installed the custom installation package.
13. You or the computer users must restart the client computers.

    See "Restarting client computers" on page 153.

14 Confirm the status of the deployed clients.

15 See "Viewing client inventory" on page 73.

About reinstalling client protection

Reinstalling client protection lets you change the protection technologies that were deployed on a computer. For example, suppose you deployed Network Threat Protection on a computer and then decided that you did not want the protection. To remove Network Threat Protection from the computer, you reinstall the protection technologies.

You may reinstall client protection by using the following deployment methods:

- Email Notification Installation
  See "Deploying clients by using Email Notification Installation" on page 49.
- Remote Push Installation
  See "Deploying clients by using Remote Push Installation" on page 50.
- Custom Installation
  See "Deploying clients by using Custom Installation" on page 51.

Installing an unmanaged computer

Unmanaged computers do not use Symantec Protection Center. Unmanaged computers are self-managed; you or the primary computer users must administer the computers. In most cases, unmanaged computers connect to your network intermittently or not at all.

Since unmanaged computers are self-managed, you or the primary computer users must maintain the computers. This maintenance includes monitoring and adjusting the protection on the computers, and updating security policies, virus definitions, and software.

To install an unmanaged computer

1 On the computer, insert the product disc.

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

2 Click **Install an unmanaged client**, and then click **Next**.

3 On the License Agreement Panel, click **I accept the terms in the license agreement**, and then click **Next**.

4 Confirm that the unmanaged computer is selected, and then click **Next**.

This panel appears when you install the client software for the first time on a computer.

5 On the Protection Options panel, select the protection types, and then click **Next**.

See "About the client installation settings" on page 47.

6 On the Ready to Install the Program panel, click **Install**.

7 On the Wizard Complete panel, click **Finish**.

Uninstalling the client

You uninstall the Symantec Endpoint Protection Small Business Edition client by using the Windows Add or Remove Programs utility.

If the client software uses a policy that blocks hardware devices, the devices are blocked after you uninstall the software. Use the Windows Device Manager to unblock the devices.

See your Windows documentation for more information.

To uninstall the client

1 On the client computer, on the Start menu, click **Control Panel > Add or Remove Programs**.

2 In the Add or Remove Programs dialog box, select **Symantec Endpoint Protection**, and then click **Remove**.

3 Follow the onscreen prompts to remove the client software.

Chapter 6

Migrating to Symantec Endpoint Protection Small Business Edition

This chapter includes the following topics:

About migrating to Symantec Endpoint Protection Small Business Edition

Symantec Endpoint Protection Small Business Edition detects and migrates Symantec legacy virus protection software.

Table 6-1 Supported migrations

Product	Description
Symantec legacy virus protection software	You can optionally migrate Symantec legacy virus protection software. Migration detects and migrates installations of the following Symantec legacy virus protection software: ■ Symantec AntiVirus Corporate Edition 9.x and 10.x ■ Symantec Client Security 2.x and 3.x See "Migrating legacy installations" on page 56. You may skip migration as follows: ■ Uninstall the Symantec legacy virus protection software from your servers and client computers. ■ During Symantec Protection Center installation, cancel the migration option. ■ After initial product installation, use Symantec Protection Center to adjust the group settings and policy settings. ■ Install the Symantec Endpoint Protection Small Business Edition client on the unprotected legacy computers.
Symantec Endpoint Protection Small Business Edition	Installation detects and upgrades Symantec Endpoint Protection Small Business Edition to a new maintenance release. See "Upgrading Symantec Endpoint Protection Small Business Edition" on page 59.
Symantec Endpoint Protection client	You can install Symantec Endpoint Protection Small Business Edition client on the computers that currently run Symantec Endpoint Protection client 11.x (enterprise edition). See "Installing the Symantec Endpoint Protection Small Business Edition client" on page 45.

Migrating legacy installations

You can optionally migrate the computers that run Symantec legacy virus protection software. During migration, the database in Symantec Endpoint Protection Small Business Edition is populated with the group data and policy data from the legacy installation. Installation packages are created for the legacy clients.

Note: Management servers migrate to clients.

Table 6-2 Migration summary

Step	Action	Description
1	Prepare the legacy installation	Prepare your legacy installation for migration as follows: ■ Disable scheduled scans. The migration might fail if a scan is running during migration. ■ Disable LiveUpdate. Conflicts might occur if LiveUpdate runs on the client computers during migration. ■ Turn off roaming service. Migration might hang and fail to complete if the roaming service is running on the client computers. ■ Unlock server groups. Unpredictable results might occur if the server groups are locked. ■ Turn off Tamper Protection. Tamper Protection can cause unpredictable results during migration. ■ Uninstall and delete reporting servers. Uninstall the reporting servers, and optionally delete the database files. See your Symantec legacy virus protection software documentation for more information.
2	Migrate legacy group and policy settings	Migrate the legacy group settings and policy settings. See "About migrating computer groups" on page 58. See "Migrating group settings and policy settings" on page 58.
3	Verify migrated data	Verify and optionally adjust the migrated group settings and policy settings. See "Viewing assigned computers" on page 81. See "Moving a computer" on page 82. See "Viewing assigned policies" on page 84. See "About adjusting the protection scans" on page 124.
4	Import legacy license	Import your legacy license file into Symantec Endpoint Protection Small Business Edition. See "Importing a license" on page 107.
5	Deploy the client software	Deploy the client to the legacy computers. See "About deploying clients" on page 48.

About migrating computer groups

Migration creates a My Company child group for each legacy group. The My Company child group name is a concatenation of each legacy group and its legacy child groups.

For example, suppose the legacy group Clients contains the legacy child groups ClientGroup1 and ClientGroup2. The My Company child group names are Clients, Clients.ClientGroup1, and Clients.ClientGroup2.

See "About computer groups" on page 81.

Migrating group settings and policy settings

The following procedure uses the Migration Wizard to migrate the group settings and the policy settings from Symantec AntiVirus Corporate Edition and Symantec Client Security.

The Migration Wizard automatically runs during initial product installation. You can also run the Migration Wizard from the Start menu on the computer that hosts Symantec Protection Center.

See "About the installation wizards" on page 32.

To migrate group settings and policy settings

1. Start the Migration Wizard if necessary.

   To start the Migration Wizard from the console computer, on the Start menu, click **All Programs > Symantec Protection Center > Symantec Protection Center Tools > Migration Wizard**.

2. In the Migration Wizard panel, click **Next**.

3. In the Migration Wizard panel, specify the following settings:

Server policy settings	Specify where the server policy settings are configured. Select one of the following options: ■ Server group ■ Each parent server
Client policy settings	Specify where the client policy settings are configured. Select one of the following options: ■ Server group or client group ■ Each parent server

4. Click **Next**.

5 In the Migration Wizard panel, select one of the following options:

Auto-detect Servers	This option imports the settings from all the servers. Type the IP address of a computer that runs the Symantec System Center.
Add Server	This option imports the settings from a single server and the clients that it manages. Type the IP address of a computer that runs a server.

6 Click **Next**.

7 Follow the on-screen prompts to complete the migration.

Upgrading Symantec Endpoint Protection Small Business Edition

Table 6-3 summarizes the steps that you follow to upgrade Symantec Endpoint Protection Small Business Edition to a new maintenance release.

Table 6-3 Upgrade summary

Step	Action	Description
Step 1	Back up the database	Back up the database before you upgrade the software.
Step 2	Stop the Symantec Protection Center service	Stop the Symantec Protection Center service before you upgrade the software. You use Windows Administrative Tools to stop the Symantec Protection Center service. You stop the Symantec Protection Center service as follows: ■ On the computer that hosts Symantec Protection Center, on the Start menu, click Settings > Control Panel > Administrative Tools > Services. ■ Select Symantec Protection Center. ■ Click Stop. ■ Close the Services window.
Step 3	Upgrade the Symantec Protection Center software	Installation automatically detects and upgrades the server software and the client software to a new maintenance release. See "Installing the server and the console" on page 35. See "About deploying clients" on page 48.

Table 6-3 Upgrade summary *(continued)*

Step	Action	Description
Step 4	Confirm the upgrade	You can confirm that the upgrade completed successfully by verifying the version number of the client software that appears in the About dialog box.

Chapter 7

Starting the Symantec Protection Center console

This chapter includes the following topics:

About starting the Symantec Protection Center console

The first time the console starts after installation, you are presented with a Welcome screen.

Table 7-1 Welcome screen options

Option	Description
Take the tour	View a tutorial about Symantec Endpoint Protection Small Business Edition.

Table 7-1 Welcome screen options *(continued)*

Option	Description
Activate your product	Register your product license serial number. Your installation of Symantec Endpoint Protection Small Business Edition includes a 30-day trial license. During those 30 days, you have access to all the product features and functions. At the end of the 30 days, you must purchase and register a license. If you already purchased a license, you may register the license serial number now. Click Activate your product to register the serial number. See "Registering a serial number" on page 106. If you have not purchased a license for Symantec Endpoint Protection Small Business Edition, contact your Symantec reseller.
Change email and proxy server settings	Optionally change the email settings that were established during installation. See "Modifying email server settings" on page 156.

About the console

The Symantec Protection Center console provides a graphical user interface for administrators. You use the console to manage policies and computers, monitor endpoint protection status, and create and manage administrator accounts.

See "Logging on to the console" on page 62.

Logging on to the console

You log on to the Symantec Protection Center console using your administrator account.

You can also log on to the console using the default administrator account that was created during installation. The user name for the default administrator account is admin. Your company's administrator selected the password.

Administrator accounts are automatically locked after five failed logon attempts. The account is locked for 15 minutes.

To log on to the console

1. Log on to the computer where Symantec Protection Center is installed.
2. On the desktop, on the Start menu, click **All Programs > Symantec Protection Center > Symantec Protection Center console**.
3. In the Login dialog box, type your user name and password.

   If you want the computer to remember your password, check **Remember me on this computer**. You will not have to type your password the next time you log on to the console.
4. Click **Log On**.

Logging on to a remote console

Symantec Endpoint Protection Small Business Edition gives you the flexibility to manage your client computers remotely. Using a remote computer that runs the console software, you can access Symantec Protection Center while you are away from the office.

The requirements for remote management are as follows:

- You must know the IP address or the host name of the computer that runs Symantec Protection Center. The IP address and the host name are available on the console Admin page.
  Click Help for information about finding the server host name and IP address.
  See "Finding the server host name and IP address" on page 156.
- The remote computer must run the console software. The console software is automatically installed during logon.
- The remote computer requires Java Runtime Environment. Java Runtime Environment automatically installs if the remote computer does not run the correct version. You might have to adjust your Internet Explorer settings for ActiveX and Java to permit installation.
- The remote computer must have Active X and scripting enabled.
- You must have an administrator account.

To log on to a remote console

1. In the Internet Explorer window, in the Address box, type the following identifier for the computer that runs Symantec Protection Center:

   http://*host name*:9090

   where *host name* is the host name or IP address of the computer that runs Symantec Protection Center. The console uses the default port 9090.

2. In the Symantec Protection Center download window, click the link to download the Symantec Protection Center console software.

   If the console software is not installed on the remote computer, the installation begins automatically. Follow the on-screen prompts to install the software.

3. In the Login dialog box, type your user name and password, and then click **Log On**.

4. If a message warns you of a host name mismatch, click **Yes**.

   The remote console URL that you specified does not match the Symantec Endpoint Protection Small Business Edition certificate name. This problem occurs if you log on and specify an IP address rather than the server computer name.

Resetting a forgotten password

You can reset your password. A new password is sent to the email address that is listed for your account. As a security precaution, you should change the new password after you receive it.

See "Editing an administrator account" on page 145.

To reset a forgotten password

1. In the Login dialog box, click **Forgot your password?**.
2. In the Forgot Password dialog box, type the user name for the account.
3. Click **New Password**.

What you can do from the console

The Symantec Protection Center console divides the functions and tasks that you perform by pages.

Table 7-2 Symantec Protection Center console pages

Page	Description
Home	Display the security status of your network. You can do the following tasks from the Home page: ■ Obtain a count of detected viruses and other security risks. ■ Obtain a count of unprotected computers in your network. ■ Obtain a count of computers that received virus definition and other content updates. ■ View license status. ■ Adjust console preferences. ■ Get information about the latest Internet and security threats.
Monitors	Monitor event logs that concern Symantec Protection Center and your managed computers. You can do the following tasks from the Monitors page: ■ View risk distribution graphs. ■ View event logs. ■ View the status of recently issued commands. ■ View and create notifications.
Reports	Run reports to get up-to-date information about computer and network activity. You can do the following tasks from the Reports page: ■ Run Quick Reports. ■ Run the Daily Summary Report. ■ Run the Weekly Summary Report.
Policies	Display the security policies that define the protection technology settings. You can do the following tasks from the Policies page: ■ View and adjust the protection settings. ■ Create, edit, copy, and delete security policies. ■ Assign security policies to computer groups. ■ Configure client computers for LiveUpdate.

Table 7-2 Symantec Protection Center console pages *(continued)*

Page	Description
Computers	Manage computers and groups. You can do the following tasks from the Computers page: ■ Create and delete groups. ■ Edit group properties. ■ View the security policies that are assigned to groups. ■ Run commands on groups. ■ Deploy the client software to computers in your network.
Admin	Manages Symantec Protection Center settings, licenses, and administrator accounts You can do the following tasks from the Admin page: ■ Create, edit, and delete administrator accounts. ■ View and edit email and proxy server settings. ■ Import and purchase licenses. ■ Adjust the LiveUpdate schedule. ■ Download content updates from LiveUpdate. ■ View LiveUpdate status and recent downloads.
Support	Displays the Symantec Support Web site.

Configuring console preferences

Preferences are your preferred settings for reports, event logs, and security status thresholds.

You can configure the following settings:

- Security status thresholds.
  These settings include the percentage of the computers that report out-of-date virus definitions and Intrusion Prevention signatures.
- Home page and Monitors page.
  These settings include auto-refresh rate and time range.
- Report settings and event log settings.
  These settings include date format and event log size.

To configure console preferences

1. In the console, click **Home**.
2. On the Home page, click **Preferences**.

   The Preferences link is in the top left Security Status pane.
3. Adjust the settings.
4. Click **OK**.

Chapter 8

Monitoring endpoint protection

This chapter includes the following topics:

About monitoring endpoint protection

The Symantec Protection Center console provides a comprehensive view of your endpoint protection.

Table 8-1 Endpoint protection monitoring

Status	Description
License	You can obtain the following license information: ■ License serial number, seat count, expiration date ■ Number of valid seats ■ Number of deployed seats ■ Number of expired seats ■ Number of over-deployed seats See "Checking license status" on page 105. See "Viewing the Weekly Status Report" on page 71.
Groups and policies	You can answer the following questions about your groups: ■ Which computers are assigned to my groups? ■ Which policies are assigned to my groups? See "Viewing assigned computers" on page 81. See "Viewing assigned policies" on page 84.
Client computers	You can answer the following questions about your client computers: ■ How many computers are managed? ■ How many computers are offline? ■ How many computers have Auto-Protect disabled? ■ How many computers have out-of-date virus definitions? ■ Which computers are infected? ■ Which computers need scanning? ■ What risks were detected in the network? See "Viewing system protection" on page 72. See "Viewing client inventory" on page 73. See "Finding unscanned computers" on page 73. See "Viewing the Daily Status Report" on page 71. See "Viewing the Weekly Status Report" on page 71. See "Viewing risks" on page 74.

Table 8-1 Endpoint protection monitoring *(continued)*

Status	Description
Events	Events are the informative, notable, and critical activities that concern Symantec Protection Center and your client computers. The event logs supplement the information is that is contained in the reports. See "Viewing the Computer Status Log" on page 76. See "Viewing the Network Threat Protection Log" on page 76. See "Viewing the TruScan Proactive Threat Scan Log" on page 77.

Viewing the Daily Status Report

The Daily Status Report provides the following information:

- Virus detection counts for cleaned, suspicious, blocked, quarantined, and deleted actions
- Virus definition distribution timeline
- Top ten risks and infections

To view the Daily Status Report

1. In the console, click **Home**.
2. On the Home page, in the Favorite Reports pane, click **Symantec Endpoint Protection Daily Status**.

Viewing the Weekly Status Report

The Weekly Status Report provides the following information:

- Computer status
- Virus detection
- Protection status snapshot
- Virus definition distribution timeline
- Risk distribution by day
- Top ten risks and infections

To view the Weekly Status Report

1. In the console, click **Home**.
2. On the Home page, in the Favorite Reports pane, click **Symantec Endpoint Protection Weekly Status**.

Viewing system protection

System protection comprises the following information:

- The number of computers with up-to-date virus definitions.
- The number of computers with out-of-date virus definitions.
- The number of computers that are offline.
- The number of computers that are disabled.

To view system protection

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

   System protection is shown in the Endpoint Status pane.
2. In the Endpoint Status pane, click **View Details** to view more system protection information.

Viewing virus and risk activity

You can view a timeline of the virus and risk activity in your network.

Virus and risk activity comprises the following information:

- The number of viruses and risks that were cleaned or blocked.
- The number of viruses and risks that were deleted.
- The number of viruses and risks that were quarantined.
- The number of viruses and risks that were detected as suspicious.

To view virus and risk activity

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

  A timeline of the virus and risk activity is shown in the Virus and Risk Activity Summary pane.

Viewing client inventory

You can confirm the status of your deployed client computers.

To view client inventory

1. In the console, click **Reports**.
2. On the Quick Reports tab, specify the following information:

Report type	You select Computer Status.
Select a report	You select Client Inventory Details.

3. Click **Create Report**.

Finding unscanned computers

You can list the computers that need scanning.

To find unscanned computers

1. In the console, click **Reports**.
2. On the Quick Reports tab, specify the following information:

Report type	You select Scan.
Selected report	You select Computers Not Scanned.

3. Click **Create Report**.

Finding offline computers

You can list the computers that are offline.

To find offline computers

1. In the console, click **Home**.
2. On the Home page, in the Endpoint Status pane, click the link that represents the number of offline computers.
3. To get more information about offline computers, click the **View Details** link.

Viewing risks

You can get information about the risks in your network.

To view infected and at risk computers

1. In the console, click **Reports**.
2. On the Quick Reports tab, specify the following information:

Report type	You select Risk.
Selected report	You select Infected and At Risk Computers.

3. Click **Create Report**.

To view newly detected risks

1. In the console, click **Reports**.
2. On the Quick Reports tab, specify the following information:

Report type	You select Risk.
Selected report	You select New Risks Detected in the Network.

3. Click **Create Report**.

To view a comprehensive risk report

1. In the console, click **Reports**.
2. On the Quick Reports tab, specify the following information:

Report type	You select Risk.
Select a report	You select Comprehensive Risk Report.

3. Click **Create Report**.

Viewing attack targets and sources

You can view attack targets and sources.

To view the top targets that were attacked

1 In the console, click **Reports**.

2 On the Quick Reports tab, specify the following information:

Report type	You select Network Threat Protection.
Select a report	You select Top Targets Attacked.

3 Click **Create Report**.

To view top attack sources

1 In the console, click **Reports**.

2 On the Quick Reports tab, specify the following information:

Report type	You select Network Threat Protection.
Select a report	You select Top Sources of Attack.

3 Click **Create Report**.

A full report contains the following statistics:

- Top attack types
- Top targets of attack
- Top sources of attack
- Top traffic notifications

To view a full report on attack targets and sources

1 In the console, click **Reports**.

2 On the Quick Reports tab, specify the following information:

Report type	You select Network Threat Protection.
Select a report	You select Full Report.
Configure option	You can optionally select the reports to include in the full report.

3 Click **Create Report**.

About events and event logs

Events are the informative, notable, and critical activities that concern Symantec Protection Center and your client computers. The client computers send the events to the server. The server stores the events in logs. The console lets you view details of the event logs.

The Monitors page displays the events that were reported to Symantec Protection Center from your entire managed client computer deployment.

The event logs supplement the information is that is contained in the reports.

Viewing the Computer Status Log

The Computer Status Log contains the events that concern the real-time operational status of your computers.

You can use the Computer Status Log to answer the following questions about your computers:

- Which protection technologies are enabled?
- Which Symantec virus definition version is installed?
- What was the last scan date?
- What was the last checkin date?

See "Restarting client computers" on page 153.

To view the Computer Status Log

1. In the console, click **Monitors**.
2. On the Monitors page, on the Logs tab, in the Log type box, select **Computer Status**.
3. Click **View Log**.

Viewing the Network Threat Protection Log

The Network Threat Protection Log contains the events that concern firewall traffic and intrusion prevention attacks.

To view the Network Threat Protection Log for the firewall traffic

1. In the console, click **Monitors**.
2. On the Monitors page, on the Logs tab, in the Log type box, select **Network Threat Protection**.

3 On the Logs tab, in the Log content box, select **Traffic**.

4 Click **View Log**.

To view the Network Threat Protection Log for the intrusion prevention attacks

1 In the console, click **Monitors**.

2 On the Monitors page, on the Logs tab, in the Log type box, select **Network Threat Protection**.

3 On the Logs tab, in the Log content box, select **Attacks**.

4 Click **View Log**.

Viewing the TruScan Proactive Threat Scan Log

You can use the TruScan Proactive Threat Scan Log to determine which applications were labeled as risks.

To view the TruScan Proactive Threat Scan Log

1 In the console, click **Monitors**.

2 On the Monitors page, on the Logs tab, in the Log type box, select **TruScan Proactive Threat Scan**.

3 Click **View Log**.

Chapter 9

Managing security policies and computer groups

This chapter includes the following topics:

About managing security policies and computer groups

In Symantec Protection Center, you manage groups of managed computers as a single unit. You manage security policies individually, and then assign the policies to groups.

Table 9-1 Policy and group management

Task	Description
Learn about Symantec security policies	The Symantec security policies define the protection technologies that protect your computers from known and unknown threats. Become familiar with the policies. Review the default protection for each policy protection type. See "About the security policies" on page 82.
Review computer groups	You organize computers with similar security needs into groups. Review the groups. Create the groups that match your organizational structure. See "About computer groups" on page 81. See "Creating a group" on page 81.
Adjust security policy settings	Symantec Endpoint Protection Small Business Edition protects your computers out-of-the-box. You do not have to adjust the policy settings unless you want to modify the out-of-the-box protection. See "About managing protection scans" on page 111. See "About managing firewall protection" on page 127. See "About managing Intrusion Prevention protection" on page 137. You can optionally allow computer users to modify the protection on their computers. See "Locking and unlocking policy settings" on page 86. Symantec recommends that you test a security policy before you use it in a production environment. See "Testing a security policy" on page 87.
Review policy assignments	You assign a policy to a computer through a group. Every group has exactly one policy of each protection type that is assigned to it at all times. See "How policies are assigned to groups" on page 86. See "Moving a computer" on page 82.

You or the computer users manage unmanaged computers. Unmanaged computers do not communicate with Symantec Protection Center to get security policies.

You can convert the computers that were installed as unmanaged computers to managed computers.

See "Converting an unmanaged computer" on page 154.

About computer groups

You organize computers with similar security needs into groups. For example, you might organize the computers in your accounting department into the Accounting group. The group structure that you define most likely matches the structure of your organization.

The Symantec Protection Center console contains the following default groups:

- The My Company group is the top-level, or parent, group. It contains a flat tree of child groups. The child group structure matches the organizational structure of your company.
- The Laptops and Desktops group contains portable computers and desktop computers. The Laptops and Desktops group is a child group under the My Company parent group.
- The Servers group contains the computers that run a supported Windows Server operating system. The Servers group is a child group under the My Company parent group.

You can place your client computers in the Laptops and Desktops group, the Servers group, or a group that you defined.

You cannot rename or delete the default groups.

Viewing assigned computers

You can verify that your computers are assigned to the correct groups.

To view assigned computers

1. In the console, click **Computers**.
2. On the Computers page, on the Computers tab, click a group.

Creating a group

Newly created groups are listed as child groups under the My Company parent group.

To create a group

1. In the console, click **Computers**.
2. On the Computers page, under Tasks, click **Add a group**.

3 In the Add Group for My Company dialog box, specify the following information:

Group Name	Type the group name. Click Help for more information about group names.
Description	Type a description of the group

4 Click **OK**.

Blocking a group

Blocking a group prevents client computers from being added to the group.

To block a group

1 In the console, click **Computers**.

2 On the Computers page, on the Computers tab, select a group, and then right-click **Edit properties**.

3 In the Group Properties dialog box, check **Block New Clients**.

4 Click **OK**.

Moving a computer

If your computers are not in the correct group, you can move them to another group.

To move a computer to another group

1 In the console, click **Computers**.

2 On the Computers page, on the Computers tab, select a group.

3 On the Computers tab, in the selected group, select the computer, and then right-click **Move**.

Use the Shift key or the Control key to select multiple computers.

4 In the Move Clients dialog box, select the new group.

5 Click **OK**.

About the security policies

The security policies define the protection technologies that protect your computers from known and unknown threats.

Table 9-2 lists the types of security policies that are included with Symantec Endpoint Protection Small Business Edition. A default policy is provided for each type.

Table 9-2 Security policy types

Policy type	Description
Virus and Spyware Policy	The Virus and Spyware Policy provides the following protection: ■ Detect, remove, and repair the side effects of known viruses, worms, Trojan horses, and blended threats. ■ Detect, remove, and repair the side effects of known spyware, adware, remote access programs, dialers, hacking tools, and joke programs. ■ TruScan proactive threat scans analyze applications and processes for behavior anomalies, to detect unknown threats and security risks. See "About managing protection scans" on page 111.
Centralized Exceptions Policy	The Centralized Exceptions Policy lists the applications and processes that are excluded from the Auto-Protect and TruScan scans. See "About exceptions" on page 125.
Firewall Policy	The Firewall Policy provides the following protection: ■ Block unauthorized users from accessing the computers and networks that connect to the Internet. ■ Detect hacker attacks. ■ Eliminate unwanted sources of network traffic. See "About managing firewall protection" on page 127.
Intrusion Prevention Policy	The Intrusion Prevention Policy automatically detects and blocks network attacks. See "About managing Intrusion Prevention protection" on page 137.
LiveUpdate Policy	The LiveUpdate Policy lists the settings that client computers use to download content updates from LiveUpdate. See "About managing content updates from LiveUpdate" on page 89.

You can increase or decrease the protection on your computers by modifying the security policies.

See "Adjusting a policy" on page 84.

You can create copies of the security policies and then customize the copies for your specific needs. You can export the security policies for use at another site that runs Symantec Endpoint Protection Small Business Edition. You can import the security policies from another site that runs Symantec Endpoint Protection Small Business Edition.

See the Help for more information on security policies.

Viewing assigned policies

You can verify that your security policies are assigned to the correct groups.

See "How policies are assigned to groups" on page 86.

Click Help for more information about the assigned policies.

To view assigned policies

1. In the console, click **Computers**.
2. On the Computers page, on the Policies tab, in the group tree, click a group.

   The policies that are assigned to the selected group are shown. Click a policy to view the settings. Click **Tasks** for more options.

Adjusting a policy

You can increase or decrease the protection on your computers by modifying the security policies.

You do not have to reassign a modified policy unless you change the group assignment.

To adjust a policy

1. In the console, click the **Policies** page.
2. On the Policies page, edit a policy.
3. Adjust the policy settings to increase or decrease protection.
4. Click **OK** to save the policy.

As an example, you can modify the default Virus and Spyware Policy to scan files on remote computers.

To adjust the default Virus and Spyware Policy

1. In the console, click **Policies**.
2. On the Policies page, click **Virus and Spyware**.
3. On the Policies page, select the Virus and Spyware Policy, and then right-click **Edit**.
4. In the policy, on the File System Auto-Protect pane, on the Scan Details tab, check **Scan files on remote computers**.
5. Click **OK**.

Creating a policy

You can create multiple versions of each type of policy. The policies that you create are stored in the database.

Symantec recommends that you test a new policy before you use it in a production environment.

See "Testing a security policy" on page 87.

To create a new policy

1. In the console, click **Policies**.
2. On the Policies page, select a policy type, and then click the link to add a new policy.
3. Modify the policy settings to increase or decrease protection.
4. Click **OK** to save the policy.
5. Optionally assign the new policy to a group.

   You can assign a new policy to a group during or after policy creation. The new policy replaces the currently assigned policy of the same protection type.

   See "How policies are assigned to groups" on page 86.

As an example, you can create a custom Virus and Spyware Policy for your Marketing department. The custom policy is based on the default Virus and Spyware Policy.

To create a custom Virus and Spyware Policy

1. In the console, click **Policies**.
2. On the Policies page, click **Virus and Spyware**.
3. On the Policies page, under Tasks, click **Add a Virus and Spyware Policy**.

4 In the policy, on the Overview pane, specify the following information:

Policy Name	Type **Virus and Spyware for Marketing**.
Description	Type **Custom policy for the Marketing department**.

5 In the policy, on the File System Auto-Protect pane, check **scan files on remote computers**.

6 Click **OK**.

Locking and unlocking policy settings

You can lock and unlock policy settings. Computer users cannot change locked policy settings. A padlock icon appears next to a lockable policy setting.

To lock or unlock a policy setting

1 In the console, click **Policies**.

2 On the Policies page, select a policy, and then right-click **Edit**.

3 Click a padlock icon to lock or unlock the corresponding setting.

4 Click **OK**.

How policies are assigned to groups

You assign a policy to a computer through a group. Every group has exactly one policy of each protection type that is assigned to it at all times.

See "About the security policies" on page 82.

See "Assigning a policy to a group" on page 87.

Policies are assigned to computer groups as follows:

- At initial installation, the Symantec default security policies are assigned to the My Company parent group.
- The security policies in the My Company parent group are automatically assigned to each newly created child group.
- You replace a policy in a group by assigning another policy of the same type. You can replace a policy that is assigned to the My Company parent group or to any child group.

How computers get policy updates

Computers get security policy updates from Symantec Protection Center. When you update a security policy by using the console, the computers receive the updates immediately.

See "About the security policies" on page 82.

Assigning a policy to a group

You can assign a policy to one or more groups. The policy replaces the currently assigned policy of the same protection type.

See "How policies are assigned to groups" on page 86.

To assign a policy to a group

1. In the console, click **Policies**.
2. On the Policies page, select a policy, and then click **Assign the policy**.
3. In the Assign policy dialog box, select the groups, and then click **Assign**.

Testing a security policy

Symantec recommends that you test a policy before you use it in a production environment.

To test a policy

1. Create a group to use for policy testing.
2. Assign the test policy to the test group.
3. Identify three or four managed computers to use for policy testing.

   If necessary, install the client software on the computers. Install the computers as managed computers.
4. Move the test computers to the test group.
5. Exercise the test computers to verify that they operate correctly.

Chapter 10

Managing content updates from LiveUpdate

This chapter includes the following topics:

About managing content updates from LiveUpdate

You manage content updates from LiveUpdate on the Policies page and the Admin page.

Table 10-1 Content update management

Task	Description
Run LiveUpdate after installation	After you install Symantec Protection Center, run LiveUpdate to download the latest virus definitions and product updates. See "Manually downloading content updates to Symantec Protection Center" on page 94.

Table 10-1 Content update management *(continued)*

Task	Description
Decide how computers get updates	Client computers automatically download virus definitions and other product updates from Symantec Protection Center. You can allow users who travel with portable computers to get updates directly from LiveUpdate by using the Internet. See "How clients receive content updates" on page 90.
Review LiveUpdate schedules	Review the default schedules that Symantec Protection Center and the client computers use to get content updates. You can adjust the schedules. See "About the default LiveUpdate schedules" on page 91. See "Configuring LiveUpdate for the server" on page 92. See "Enabling LiveUpdate for clients" on page 92.
Manage server downloads	Manage the content updates that are downloaded to Symantec Protection Center. See "Viewing LiveUpdate downloads" on page 93. See "Checking LiveUpdate server activity" on page 93. See "Manually downloading content updates to Symantec Protection Center" on page 94.

About LiveUpdate

LiveUpdate provides continuous product support by downloading virus definitions and product updates.

Downloading virus definitions do not require a computer restart. Downloading product updates might require a computer restart.

See "How clients receive content updates" on page 90.

How clients receive content updates

Your client computers automatically download virus definitions and other product updates from Symantec Protection Center.

Users who travel with the portable computers that connect intermittently or not at all to your network cannot get updates from Symantec Protection Center. In this case, you can allow the client computers to get updates directly from LiveUpdate by using the Internet.

See "Enabling LiveUpdate for clients" on page 92.

A client computer receives the content updates from LiveUpdate in the following situations:

- LiveUpdate scheduling is enabled for the client computer.
- The client computer's virus definitions are old. The client computer is unable to communicate with Symantec Protection Center.
- The client computer has repeatedly failed to communicate with Symantec Protection Center.
  A portable computer might be unable to communicate with the server because it is disconnected from the network.

The computer does not receive the content updates from LiveUpdate when the virus definitions are current and the computer can communicate with Symantec Protection Center.

About the default LiveUpdate schedules

Table 10-2 lists the default settings that Symantec Protection Center uses to download content updates from LiveUpdate. The settings are defined in the Server Properties on the Admin page.

See "Configuring LiveUpdate for the server" on page 92.

Table 10-2 Default server schedule

Setting	Description
Frequency	Symantec Protection Center gets content updates from LiveUpdate every four hours
Retry interval Retry window	Symantec Protection Center is unable to connect to LiveUpdate, it retries every 15 minutes for an hour.

Table 10-3 lists the default settings that client computers use to download content updates from LiveUpdate. The settings are defined in the LiveUpdate Policy.

See "Enabling LiveUpdate for clients" on page 92.

Table 10-3 Default client schedule

Setting	Description
Enable LiveUpdate Scheduling	Enabled If you disable this setting, client computers cannot get content updates from LiveUpdate.
Frequency	Client computers get daily content updates. The content update download begins at 9:55 PM, plus or minus two hours.
Retry Window	If a client computer is unable to get content updates, the computer keeps trying every hour for 24 hours.

Configuring LiveUpdate for the server

You can adjust the schedule that Symantec Protection Center uses to download content updates from LiveUpdate.

For example, you can change the default server schedule frequency from hourly to daily.

To configure the default server schedule frequency

1. In the console, click **Admin**.
2. On the Admin page, click **System**.
3. On the Admin page, under Tasks, click **Edit the server properties**.
4. In the Server Properties dialog box, on the LiveUpdate tab, change the frequency to daily.
5. Click **OK**.

Enabling LiveUpdate for clients

If you enable LiveUpdate for client computers, the computers get content updates from LiveUpdate, based on the default schedule or a schedule that you specify.

If you disable LiveUpdate for client computers, the computers do not get content updates from LiveUpdate.

See "How clients receive content updates" on page 90.

See "Configuring LiveUpdate for the server" on page 92.

To enable LiveUpdate for clients

1. In the console, click **Policies**.
2. On the Policies page, select the LiveUpdate Policy, and then right-click **Edit**.

3 In the LiveUpdate Policy, click **Schedule**.

4 In the LiveUpdate Policy, check **Allow LiveUpdate to run on client computers**.

5 In the LiveUpdate Policy, specify the frequency and the retry window.

6 Click **OK**.

To disable LiveUpdate for clients

1 In the console, click **Policies**.

2 On the Policies page, select the LiveUpdate Policy, and then right-click **Edit**.

3 In the LiveUpdate Policy, click **Schedule**.

4 In the LiveUpdate Policy, uncheck **Allow LiveUpdate to run on client computers**.

5 Click **OK**.

Checking LiveUpdate server activity

You can list the events that concern Symantec Protection Center and LiveUpdate. From these events, you can determine when content was updated.

To check LiveUpdate server activity

1 In the console, click **Admin**.

2 On the Admin page, under Tasks, click **System**.

3 On the Admin page, click **Show the LiveUpdate Status**.

4 Click **Close** to close the window.

Viewing LiveUpdate downloads

You can list the recent downloads of LiveUpdate content.

To view LiveUpdate downloads

1 In the console, click **Admin**.

2 On the Admin page, click **System**.

3 On the Admin page, click **Show LiveUpdate downloads**.

4 Click **Close**.

Manually downloading content updates to Symantec Protection Center

You do not have to wait for your scheduled LiveUpdate downloads. You can manually download content updates to Symantec Protection Center.

To manually download content updates to Symantec Protection Center

1. In the console, click **Admin**.
2. On the Admin page, click **System**.
3. On the Admin page, click **Download LiveUpdate Content**.
4. In the Download LiveUpdate Content dialog box, click **Download**.

Chapter 11

Managing notifications

This chapter includes the following topics:

About managing notifications

Notifications alert administrators and computer users about potential security problems.

You manage notifications on the Monitors page. You can use the Home page to determine the number of unacknowledged notifications that need your attention.

Table 11-1 Notification management

Task	Description
Learn about notifications	Learn how notifications work. See "How notifications work" on page 96.
Review preconfigured notifications	Review the preconfigured notifications that are included with Symantec Endpoint Protection Small Business Edition. See "About the default notifications" on page 96.

Table 11-1 Notification management *(continued)*

Task	Description
View unacknowledged notifications	View and respond to unacknowledged notifications. See "Viewing notifications" on page 97.
Create new notifications	Optionally create notifications to remind you and other administrators about important issues. See "Creating a notification" on page 98.
Create notification filters	Optionally create filters to expand or limit your view of notifications. See "Creating a notification filter" on page 98.

How notifications work

Notifications alert administrators and users about potential security problems. For example, a notification can alert administrators about an expired license or a virus infection.

Events can trigger a notification. A new security risk, a change to a client computer, or trialware license expiration can trigger a notification.

Actions can occur once a notification is triggered. These actions include logging the notification, running a batch file or executable file, and sending an email message.

See "About the default notifications" on page 96.

See "Creating a notification" on page 98.

About the default notifications

Several notifications are pre-configured for your use.

Click Help for more information about the default notifications.

Table 11-2 Default notifications

Notification	Description
New Client Software	The notification alerts administrators about new client software packages.

Table 11-2 Default notifications *(continued)*

Notification	Description
Paid License Issue	The notification alerts administrators about expired licenses.
Over-Deployment Issue	The notification alerts administrators about over-deployed paid licenses.
Trialware License Expiration	The notification alerts administrators about expired trial licenses.
Virus Definitions Out-of-date	The notification alerts administrators about out-of-date virus definitions. The notification is triggered when the virus definitions on three client computers are older than three days.
Risk Outbreak	The notification alerts administrators about security risk outbreaks. The notification is triggered when 10 risk outbreaks occur within 1 minute.
Server Health	The notification alerts administrators about server health issues.

Viewing notifications

You can view unacknowledged notifications or all notifications. You can view all the notifications that are configured in the console.

To view unacknowledged notifications

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

   The Home page lists the number of unacknowledged notifications.

2. On the Home page, in the Security Status pane, click **View Notifications**.

3. On the Notifications tab, in the Report column, click a document icon to obtain more information about the corresponding notification.

   The notification report appears in a separate browser window.

4. On the Notifications tab, in the Ack column, click the red icon to acknowledge a notification.

To view all notifications

1. In the console, click **Monitors**.
2. On the Monitors page, on the Notifications tab, in the Use a saved filter box, optionally select a saved filter.

   See "Creating a notification filter" on page 98.
3. On the Notifications tab, click **View Notifications**.

To view all configured notifications

1. In the console, click **Monitors**.
2. On the Monitors page, on the Notifications tab, click **Notification Conditions**.

   All the notifications that are configured in the console are shown. You can filter the list by selecting a notification type from the Show notification type menu.

Creating a notification

You can create a notification that reminds you and other administrators to perform important issues, such as renewing an expired license.

To create a notification to renew an expired license

1. In the console, click **Monitors**.
2. On the Monitors page, on the Notifications tab, click **Notification Conditions**.
3. On the Notifications tab, click **Add**, and then click **Licensing issue**.
4. In the Add Notification Condition dialog box, specify the following information:

Notification name	Type **Reminder to contact Symantec partner**.
Licensing type	Click **Paid license expiration**.
Send email to System Administrators	Check this box. Uncheck all other boxes.

5. Click **OK**.

Creating a notification filter

You use filters to expand or limit your view of notifications.

See "Viewing notifications" on page 97.

As an example, you can create a filter for unacknowledged risk outbreak notifications.

To create a notification filter

1 In the console, click **Monitors**.

2 On the Monitors page, on the Notifications tab, click **Advanced Settings**, and then specify the following filter settings:

Time range	Select Past 24 hours.
Acknowledged status	Select Not acknowledged.
Notification type	Select Risk outbreak.
Created by	Select admin.
Notification name	Select Risk Outbreak.
Limit	Accept the default.

3 Click **Save Filter**.

4 On the Notifications tab, in the Filter name box, type **Unacknowledged Risk Outbreaks**, and then click **OK**.

Chapter 12

Managing product licenses

This chapter includes the following topics:

About managing product licenses

You manage product licenses on the Admin page.

Table 12-1 License management

Task	Description
Learn how a license works	A license is a vital part of Symantec Endpoint Protection Small Business Edition. It controls your access to the software's features and functions. See "About licenses" on page 103. See "Product license requirements" on page 25.
Purchase a license	A license gives you unrestricted access to all the features and functions in Symantec Endpoint Protection Small Business Edition. You need to purchase a license in the following situations: ■ You want to purchase Symantec Endpoint Protection Small Business Edition. ■ Your trialware license expired. ■ Your paid license expired. ■ Your license is over-deployed. See "About purchasing a license" on page 105. See "About upgrading trialware" on page 108.
Register your product serial number	Registering your product serial number activates the license. You need to register your product serial number in the following situations: ■ You purchased the boxed software. ■ You purchased the product disc image. ■ You purchased a license. See "Registering a serial number" on page 106.
Import your license into the console	Importing a license saves the license file in the Symantec Protection Center database. You can import a license file that you received from sources such as the following: ■ Symantec Licensing Portal ■ Symantec partner ■ Symantec sales team ■ Symantec legacy virus protection software license See "Importing a license" on page 107.

Table 12-1 License management *(continued)*

Task	Description
Review the default license notifications	License notifications alert administrators about expired licenses and other license issues. See "About the default notifications" on page 96.
Check license status	You can obtain the status for each license that you imported into the console. See "Checking license status" on page 105.
Back up your license files	Backing up your license files preserves the license files in case the database or the computer's hard disk is damaged. See "Backing up your license files" on page 109.

About licenses

A license gives you unrestricted access to all the features and functions in Symantec Endpoint Protection Small Business Edition. A license lets you install the Symantec Endpoint Protection Small Business Edition client on a designated number of computers. A license lets you download virus definitions and product updates from LiveUpdate.

The following terminology describes licenses:

Serial number	A license contains a serial number or a renewal chain of serial numbers. A license has a start date and an expiration date.
Deployed	Deployed refers to the client software that is installed on client computers.
Seat	A seat is the right to get content on a single deployed client computer. A license is valid for a specific number of seats. Valid seats is the total number of seats in all valid licenses.
Over-deployed	A license is over-deployed when the number of deployed clients exceeds the number of licensed seats. The following equation defines over-deployed: Over-deployed = deployed - valid seats - expired licenses

You must purchase a license within 30 days of initial installation. You can purchase a license from the Symantec Business Store Web site, your Symantec partner, or

your Symantec sales team. You must purchase enough seats so that your license covers all your deployed computers.

After you purchase a license, you obtain the .slf license file from the Symantec Licensing Portal Web site, your Symantec partner, or your Symantec sales team.

About the Symantec Licensing Portal

You use the Symantec Licensing Portal to register and manage product licenses.

See the following Symantec Web site:

https://licensing.symantec.com/

You need the following items to register a license:

- Symantec Licensing Portal account
  You can visit the Symantec Licensing Portal Web site at any time to create an account.
  See "Creating a Symantec Licensing Portal account" on page 104.
- Product serial number
  You receive a product serial number when you purchase a license.
- Internet connection
  You need an Internet connection to access the Symantec Licensing Portal Web site.

Creating a Symantec Licensing Portal account

You need a Symantec Licensing Portal account to register and manage product licenses.

To create a Symantec Licensing Portal account

1. In your Web browser, go to the following Web site:

   https://licensing.symantec.com/

2. On the Symantec Licensing Portal Web site, in the Login to Your Account section, click **Create An Account**.
3. On the Symantec Licensing Portal Web site, fill in the Create An Account form, and then click **Submit**.
4. On the Symantec Licensing Portal Web site, click **I Accept** to accept the Symantec User Agreement.

5 On the Symantec Licensing Portal Web site, click the **Licensing Portal Home Page** option to display the Symantec Licensing Portal Home page.

From the Home page, you can manage your account, register serial numbers, and download license files.

6 Click **Logout** to log off the Symantec Licensing Portal Web site.

Checking license status

You can obtain the status for each paid license that you imported into the console.

See "Importing a license" on page 107.

You can obtain the following license information:

- License serial number, total seat count , expiration date
- Number of valid seats
- Number of deployed seats
- Number of seats that expire in 60 days and 30 days
- Number of expired seats
- Number of over-deployed clients

License status is not available for a trialware license.

To determine if your installation uses a paid license or a trialware license

1 In the console, click **Admin**.

2 On the Admin page, click **Licenses**.

To check license status for paid licenses

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

2 On the Home page, click **Licensing Details**.

About purchasing a license

You need to purchase a license in the following situations:

- You want to purchase Symantec Endpoint Protection Small Business Edition.
- Your trialware license expired.
- Your current license expired.
- Your license is over-deployed.

Contact your Symantec partner to purchase a license.

Registering a serial number

Registering your product serial number activates the license.

You need to register your product serial number in the following situations:

- You purchased the boxed software.
- You purchased the product disc image.
- You purchased a license to upgrade your trialware installation.
- You purchased a renewal license.
- You purchased additional licenses for deployed client computers.

Note: If you purchase software from a Symantec partner, contact the Symantec partner to obtain a license file.

You register a serial number using the Symantec Licensing Portal Web site.

See "About the Symantec Licensing Portal" on page 104.

The following procedure registers a serial number for a new purchase, and downloads the license file to your computer.

To register a serial number

1. In the console, click **Admin**.
2. On the Admin page, under Licenses, click **Register a serial number**.
3. On the Symantec Licensing Portal Web site, log on to your account or create an account if you do not have one.

   See "Creating a Symantec Licensing Portal account" on page 104.
4. Click the **Licensing Portal Home Page** option.
5. On the Symantec Licensing Portal Home page, click **New Purchase**.
6. On the Serial Number entry page, type your product serial number, and then click **Submit**.

   The serial number appears at the bottom of the page.
7. Click **Next**.

8 On the License Registration Verification page, verify your information, and then click **Complete Registration**.

Your serial number and license key appear on the License Key Confirmation page.

9 On the License Key Confirmation page, click the license key file name link to download the license file to your computer.

See "Downloading a license file" on page 108.

10 In the Save dialog box, save the license file in a directory of your choice.

Retain the directory location.

11 Click **Logout** to log off the Symantec Licensing Portal Web site.

12 Back up the license file.

See "Backing up your license files" on page 109.

13 Import the license file into the console.

See "Importing a license" on page 107.

Importing a license

Importing a license saves the license file in the Symantec Protection Center database.

You can import a license file that you received from sources such as the following:

- Symantec Licensing Portal
- Symantec partner
- Symantec sales team
- Symantec Business Store
- Symantec legacy virus protection software

To import a license

1 Save the license file on a computer or network that is accessible from the console computer.

2 In the console, click **Admin**.

3 On the Admin page, under Licenses, click **Import a license file**.

4 In the Import License dialog box, select the .slf license file.

5 Click **Import**.

About upgrading trialware

If you installed trialware, you must purchase a license. You do not need to reinstall the software.

Contact your Symantec partner to purchase a license.

See "About trialware" on page 24.

About renewing a license

Renewing a license purchases a renewal license for an expired license.

Contact your Symantec partner to renew a license.

Downloading a license file

You can download an existing license file from the Symantec Licensing Portal Web site.

Note: If you purchase software from a Symantec partner, contact the Symantec partner to obtain a copy of your license file.

To download an existing license file

1. In the console, click **Admin**.
2. On the Admin page, under Licenses, click **Register to download a license file**.
3. On the Symantec Licensing Portal Web site, log on to your account.
4. Click the **Licensing Portal Home Page** option.
5. On the Symantec Licensing Portal Home page, click **Manage Licenses**, and then click **License Catalog**.
6. In the License Catalog, click a license key file name link to download the license file to your computer.
7. In the Save dialog box, save the license file in a directory of your choice.

   Retain the directory location.
8. Click **Logout** to log off the Symantec Licensing Portal Web site.

9 Back up the license file.

See “Backing up your license files” on page 109.

10 Verify the status of the license file.

See “Checking license status” on page 105.

Backing up your license files

Symantec recommends that you back up your license files. Backing up the license files preserves the license files in case the database or the console computer's hard disk is damaged.

Your license files are located in the directory where you saved the files. If you misplaced the license files, you can download the files from the Symantec Licensing Portal Web site.

See “Downloading a license file” on page 108.

To back up your license files

- Using Windows, copy the .slf license files from the directory where you saved the files to another computer of your choice.

  See your company's procedure for backing up files.

Chapter 13

Managing protection scans

This chapter includes the following topics:

About managing protection scans

You manage protection scans on the Policies page. You can schedule protection scans to run on client computers at designated times. You can run protection scans on demand from the console. You can enable or disable TruScan proactive threat scans.

The default scan settings are defined in the following policies:

- Virus and Spyware Policy
- Virus and Spyware High Security Policy

- Virus and Spyware High Performance Policy

Table 13-1 lists suggestions for managing protection scans.

Table 13-1 Protection scan management

Task	Description
Keep virus definitions current	Make sure the latest virus definitions are installed on the client computers. See "About managing content updates from LiveUpdate" on page 89.
Scan computers	Regularly scan computers for viruses and security risks. Run the on-demand scan on newly deployed computers. See "Scanning computers" on page 122. See "About the default protection scan settings" on page 117.
Isolate infected computers	Disconnect the infected computers from the network. Blended threats such as worms can travel by shared resources without user interaction. Once the viruses are eliminated, reconnect the computers to the network.
Repair infected computers	Scan the infected computers to clean, delete, or quarantine detected risks. See "About the default protection scan settings" on page 117.
Check protection status	Ensure that Auto-Protect is enabled on the computers. Ensure that the scans run regularly by checking the last scan date. Ensure that the virus definitions are current. See "About monitoring endpoint protection" on page 69.

Table 13-1 Protection scan management *(continued)*

Task	Description
Adjust scan settings	In most cases, the default scan settings provide adequate protection for computers. If necessary, you can increase or decrease protection as follows: ■ Prevent the computer users from changing scan settings. ■ Change the time that a scan is scheduled to run. ■ Change the repair actions that occur when a virus is detected. ■ Schedule a startup scan to run when the users log on to the computers. See "About adjusting the protection scans" on page 124.
Identify scan exceptions	You can exclude a security risk or process from a protection scan. See "About exceptions" on page 125.
Manage quarantined files	You or the computer users can quarantine infected files. If a quarantined file cannot be fixed, you or the computer users must decide what to do with the infected file. See "About managing quarantined files" on page 123.
Configure exceptions	Exceptions are the known security risks and processes that you want to exclude from the protection scans. See "About exceptions" on page 125.

How protection scans work

Protection scans identify and neutralize or eliminate viruses and security risks on your computers. Protection scans examine files for the viruses that match definitions in a virus dictionary. Protection scans identify unknown behavior anomalies in applications and processes.

See "About the types of protection scans" on page 115.

Figure 13-1 Virus and Spyware Protection

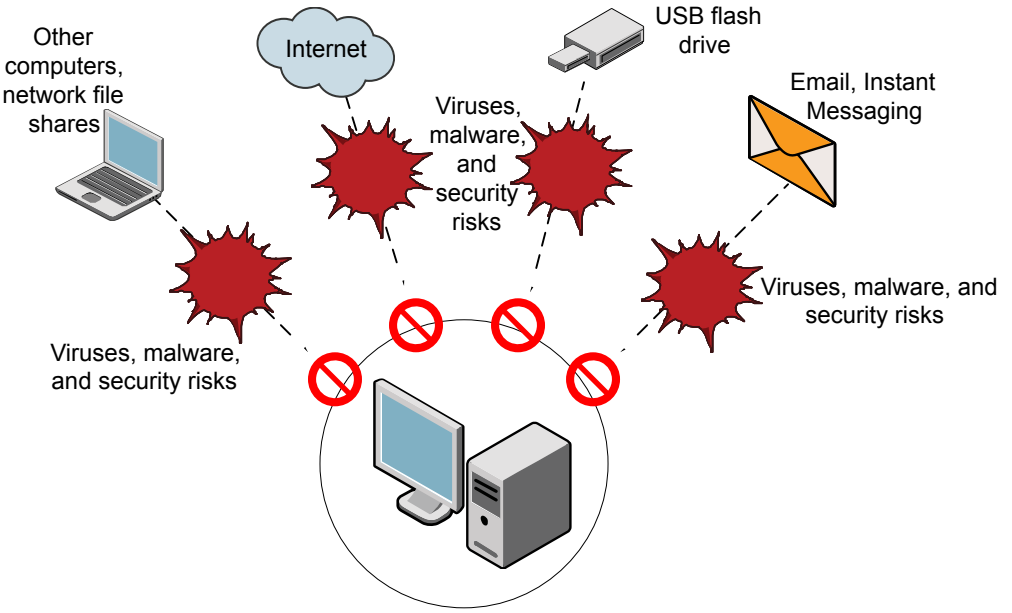


Table 13-2 lists the known viruses and security risks that protection scans detect.

Table 13-2 Known viruses and security risks

Risk	Description
Virus	A computer program that attaches to another program or document when it runs.
Malicious Internet bot	A program that runs automated tasks over the Internet for malicious purposes. A bot automates attacks on a computer or collects information from a Web site.
Worm	A program that replicates without infecting other programs. A worm spreads by copying itself from disk to disk or by replicating in memory.
Trojan horse	A malicious program that hides itself in a benign game or utility.
Blended threat	A threat that blends the characteristics of viruses, worms, Trojan horses, and code with server and Internet vulnerabilities to initiate, transmit, and spread an attack.

Table 13-2 Known viruses and security risks *(continued)*

Risk	Description
Adware	A program that secretly gathers personal information through the Internet and relays it back to another computer. An adware program is unknowingly downloaded from a Web site. It can arrive through an email message or instant messenger program.
Dialer	A program that uses a computer, without the user's permission or knowledge, to dial through the Internet to a 900 number or an FTP site.
Hacking tool	A program that is used to gain unauthorized access to a user's computer. For example, a keystroke logger tracks and records individual keystrokes.
Joke program	A program that alters or interrupts the operation of a computer in a way that is intended to be humorous or frightening.
Spyware	A program that secretly monitors system activity, and detects passwords and other confidential information.
Remote access program	A program that allows access over the Internet from another computer, to gain information or to attack or alter a user's computer.
Trackware	A program that traces a user's path on the Internet.

About the types of protection scans

Table 13-3 lists the types of protection scans.

Table 13-3 Scan types

Scan type	Description
Auto-Protect scans	Auto-Protect scans continuously inspect files and email data as they are written to or read from a computer. Auto-Protect scans automatically neutralize or eliminate detected viruses and security risks. The Auto-Protect scans are as follows: ■ File System Auto-Protect File System Auto-Protect loads at computer startup. It inspects all files for viruses and security risks, and blocks the security risks from being installed. It can optionally scan files by file extension, scan files on remote computers, and scan floppies for boot viruses. It can optionally back up files before it attempts to repair the files, and terminate processes and stop services. ■ Internet Email Auto-Protect Internet Email Auto-Protect scans the email messages that use the POP3 or SMTP communications protocol over the Secure Sockets Layer. It scans the message text and the message attachments in incoming messages and outgoing messages. ■ Microsoft Outlook Auto-Protect Microsoft Outlook Auto-Protect scans Outlook email messages. It scans the message text and the message attachments in incoming messages and outgoing messages.
Administrator-defined scans	Administrator-defined scans detect viruses and security risks by examining files and processes. Administrator-defined scans can inspect memory and load points. The administrator-defined scans are as follows: ■ Scheduled scans A scheduled scan runs on the client computers at designated times. The concurrently scheduled scans run sequentially. If a computer is turned off during a scheduled scan, the scan does not run unless it is configured to retry missed scans. You can schedule an active, full, or custom scan. ■ Startup scans and triggered scans Startup scans run when the users log on to the computers. Triggered scans run when new virus definitions are downloaded to computers. ■ On-demand scan The on-demand scan provides immediate results. The administrators can run the on-demand scan from the console.

Table 13-3 Scan types *(continued)*

Scan type	Description
TruScan proactive threat scans	TruScan proactive threat scan analyzes application behavior and process behavior. TruScan proactive threat scan determines if an application or process exhibits characteristics of known threats. This type of protection is often called protection from zero-day attacks. TruScan proactive threat scan detects characteristics of the following known threats: ■ Trojan horses ■ Worms ■ Keyloggers ■ Adware and spyware ■ Applications that are used for malicious purposes

About the default protection scan settings

The default protection scan settings are defined in three Symantec policies. The policies provide different levels of protection.

The default Virus and Spyware Policy provides a good balance between security and performance.

Table 13-4 Virus and Spyware Policy settings

Setting	Description
User locks	The following settings are locked: ■ In the scheduled scan, the setting to back up files before the files are repaired is locked. ■ In the File System Auto-Protect scan, the setting to block security risks from being installed is locked.
Group assignment	The policy is assigned to the My Company parent group at initial installation. See "How policies are assigned to groups" on page 86.

Table 13-4 Virus and Spyware Policy settings *(continued)*

Setting	Description
Auto-Protect scans	File System Auto-Protect provides the following protection: ■ Scans all files for viruses and security risks. ■ Blocks the security risks from being installed. ■ Cleans the virus-infected files. Backs up the files before it repairs them. Quarantines the files that cannot be cleaned. ■ Quarantines the files with security risks. Logs the files that cannot be quarantined. ■ Checks all floppies for boot viruses. Logs the boot viruses. ■ Notifies the computer users about viruses and security risks. Internet Email Auto-Protect provides the following protection: ■ Scans all files, including the files that are inside compressed files. ■ Cleans the virus-infected files. Quarantines the files that cannot be cleaned. ■ Quarantines the files with security risks. Logs the files that cannot be quarantined. ■ Notifies the computer users about viruses and security risks. Microsoft Outlook Auto-Protect provides the following protection: ■ Scans all files, including the files that are inside compressed files. ■ Cleans the virus-infected files. Quarantines the files that cannot be cleaned. ■ Quarantines the files with security risks. Logs the files that cannot be quarantined. ■ Notifies the computer users about viruses and security risks.
TruScan Proactive Threat Scans	Enabled

Table 13-4 Virus and Spyware Policy settings *(continued)*

Setting	Description
Administrator-defined scans	The scheduled scan provides the following protection: ■ Performs a full scan every Monday at 8:00 PM. ■ Scans all files and folders, including the files that are contained in compressed files. ■ Scans memory, common infection locations, and known virus and security risk locations. ■ Cleans the virus-infected files. Backs up the files before it repairs them. Quarantines the files that cannot be cleaned. ■ Quarantines the files with security risks. Logs the files that cannot be quarantined. ■ Retires missed scans within three days. The on-demand scan provides the following protection: ■ Scans all files and folders, including the files that are contained in compressed files. ■ Scans memory and common infection locations. ■ Cleans the virus-infected files. Backs up the files before it repairs them. Quarantines the files that cannot be cleaned. ■ Quarantines the files with security risks. Logs the files that cannot be quarantined.

The default Virus and Spyware High Security Policy provides high-level security, and includes many of the settings from the Virus and Spyware Policy. The policy provides increased scanning.

Table 13-5 Virus and Spyware High Security Policy settings

Setting	Description
User locks	Same as Virus and Spyware Policy
Group assignment	None
Auto-Protect scans	Same as Virus and Spyware Policy File System Auto-Protect inspects the files on the remote computers.
TruScan proactive threat scans	Same as Virus and Spyware Policy

Table 13-5 Virus and Spyware High Security Policy settings *(continued)*

Setting	Description
Administrator-defined scans	Same as Virus and Spyware Policy An active scan runs when new virus definitions arrive. The on-demand scan inspects the known virus and security risk locations.

The default Virus and Spyware High Performance Policy provides high-level performance. The policy includes many of the settings from the Virus and Spyware Policy. The policy provides reduced security.

Table 13-6 Virus and Spyware High Performance Policy settings

Setting	Description
User locks	Same as Virus and Spyware Policy The setting to enable or disable Internet Email Auto-Protect is locked. The setting to enable or disable Microsoft Outlook Auto-Protect is locked.
Group assignment	None
Auto-Protect scans	Same as Virus and Spyware Policy File System Auto-Protect scans common file extensions. It does not scan all files. Internet Email Auto-Protect is disabled. Microsoft Outlook Auto-Protect is disabled.
TruScan proactive threat scans	Same as Virus and Spyware Policy
Administrator-defined scans	Same as Virus and Spyware Policy The scheduled scan is a monthly full scan. It runs at 8:00 PM on the first day of each month. Missed scans are retried within 11 days.

Enabling File System Auto-Protect

If a user on a client computer disabled File System Auto-Protect, you can enable it.

To enable File System Auto-Protect

1. In the console, click **Computers**.
2. On the Computers page, on the Computers tab, select a group, right-click **Run Command on Group**, and then click **Enable Auto-Protect**.

Scheduling an administrator-defined scan

You can schedule scans to automatically run on the client computers at designated times.

See "About the types of protection scans" on page 115.

For example, you can create a daily active scan that runs at 10:00 AM each day.

To schedule an administrator-defined scan

1. In the console, click **Policies**.
2. On the Policies page, select the default Virus and Spyware Policy, and then right-click **Edit**.
3. In the policy, click **Administrator-defined Scans**.
4. In the policy, on the Scans tab, click **Add**.
5. In the policy, on the Scan Details tab, specify the following information:

Scan name	You type **Daily Scheduled Scan**.
Description	You type **This scan runs daily at 10:00 AM**.
Scan type	You select Active.

6. In the policy, on the Schedule tab, specify the following information:

Scan	You select Daily.
At	You select 10:00 AM.
Retry the scan within	You select 12 hours.

7. Click **OK**.

Scheduling a startup scan

A startup scan runs when a user logs on to a computer.

To schedule a startup scan

1. In the console, click **Policies**.
2. On the Policies page, select the Virus and Spyware Policy, and then right-click **Edit**.
3. In the policy, click **Administrator-defined Scans**.
4. In the policy, on the Advanced tab, check **Run startup scans when users log on**.
5. In the policy, on the Advanced tab, optionally check **Allow users to modify startup scans**.
6. Click **OK**.

Scheduling a triggered scan

When you schedule a triggered scan, an active scan runs when new virus definitions are downloaded to a computer.

To schedule a triggered scan

1. In the console, click **Policies**.
2. On the Policies page, select the Virus and Spyware Policy, and then right-click **Edit**.
3. In the policy, click **Administrator-defined scans**.
4. In the policy, on the Advanced tab, check **Run an Active scan when new virus definitions arrive**.
5. Click **OK**.

Scanning computers

You can scan all the computers in a selected group. You can scan a selected computer.

To scan all the computers in a group

1. In the console, click **Computers**.
2. On the Computers page, on the Computers tab, select a group, right-click **Run Command on Group**, and then click **Scan**.

To scan a selected computer

1. In the console, click **Computers**.
2. On the Computers page, on the Computers tab, select a group.
3. On the Computers tab, in the selected group, select a computer, right-click **Run Command on Clients**, and then click **Scan**.

Updating virus definitions on computers

You can update the virus definitions on a selected computer. You can update the virus definitions, and scan a selected computer.

To update virus definitions on a selected computer

1. In the console, click **Computers**.
2. On the Computers page, on the Computers tab, select a group.
3. On the Computers tab, in the selected group, select a computer, right-click **Run Command on Clients**, and then click **Update Content**.

To update virus definitions, and scan a selected computer

1. In the console, click **Computers**.
2. On the Computers page, on the Computers tab, select a group.
3. On the Computers tab, in the selected group, select a computer, right-click **Run Command on Clients**, and then click **Update Content and Scan**.

About managing quarantined files

You or the computer users can quarantine infected files. If a quarantined file cannot be fixed, you or the computer users must decide what to do with the infected file.

Suggestions for managing quarantined files are as follows:

- Delete a quarantined file if a backup file exists or a replacement file is available from a trustworthy source.
- Leave the files with unknown infections in quarantine until Symantec releases new virus definitions.
- Monitor the quarantined files.
  Periodically check the quarantined files to prevent accumulating large numbers of files. Check the quarantined files when a new virus outbreak appears on the network.

Enabling or disabling TruScan proactive threat scans

You can disable TruScan proactive threat scans. You can lock the setting so that users cannot change it.

To enable or disable TruScan proactive threat scans

1. In the console, click **Policies**.
2. On the Policies page, select the Virus and Spyware Policy, and then right-click **Edit**.
3. In the policy, click **TruScan Proactive Threat Scans**, and then uncheck **Enable TruScan Proactive Threat Scan**.
4. Optionally click the padlock icon to lock the setting.
5. Click **OK**.

About adjusting the protection scans

You can change the protection scan settings on client computers as follows:

- Set user locks.
  Lock the scan settings so that computer users cannot change them.
- Modify administrator-defined scans.
  Change the time that a scan is scheduled to run on the client computers. Schedule a startup scan to run when the users log on to the computers. Schedule a trigger scan to run when new virus definitions are downloaded to the computers.
- Modify scan options.
  Change the Auto-Protect scan options. Enable or disable the TruScan proactive threat scans.
- Modify the repair actions.
  Change the actions that occur when a virus is detected.
- Modify the backup actions.
  Back up the infected files before they are repaired.
- Modify the notify actions.
  Configure a message to appear on the client computers when a virus is detected. Configure a notification to trigger when a virus is detected.
- Modify exceptions.
  Exclude security risks and processes from the protection scans. Control the types of exceptions that computer users can specify.

About exceptions

Exceptions are known security risks and processes you want to exclude from the protection scans. In some cases, exceptions can reduce scan time and increase system performance.

You specify exceptions in the Centralized Exceptions Policy.

Click Help for more information about configuring exceptions.

Table 13-7 lists the types of exceptions that you can exclude from the protection scans.

Table 13-7 Exception types

Type	Description
Security risk exceptions	You can exclude the following security risks: ■ Known security risks ■ Files ■ Folders ■ Extensions
TruScan proactive threat scan exceptions	You can exclude processes from the TruScan proactive threat scans. You can specify the action to take for a known process that the TruScan proactive threat scans detect. You can force the detection of a process.
Tamper Protection exception	You can exclude files from Tamper Protection. Tamper Protection provides real-time protection for Symantec applications that run on the server and the client computers. Tamper Protection prevents non-Symantec processes from affecting Symantec processes. See the Help on the client computer for more information about Tamper Protection.

You can use the Centralized Exceptions Policy to control the type of exceptions that computer users can specify.

You can allow computer users to specify the following exceptions:

- Security risk
- File
- Folder
- Extension

- TruScan proactive threat scan

Configuring an exception

Exceptions are the known security risks and processes that you want to exclude from the protection scans.

To configure an exception

1. In the console, click **Policies**.
2. On the Policies page, select the Centralized Exceptions policy, and then right-click **Edit**.
3. In the policy, click **Centralized Exceptions**.
4. In the policy, click **Add > Security Risk Exceptions > Known Risks**.
5. In the Add Known Security Risk Exceptions dialog box, check the security risks that you want to exclude from the protection scans.
6. In the Add Known Security Risk Exceptions dialog box, optionally check **Log when the security risk is detected**.
7. Click **OK**.

Chapter 14

Managing firewall protection

This chapter includes the following topics:

About managing firewall protection

You manage firewall protection on the Policies page.

Table 14-1 Firewall protection management

Task	Description
Read about firewall protection	Learn about how firewall protection works. See "How the firewall works" on page 128.

Table 14-1 Firewall protection management *(continued)*

Task	Description
Enable firewall protection	You can enable the default firewall protection or the custom firewall protection. See "About the default firewall protection" on page 133. See "Enabling firewall protection" on page 134. See "Adjusting the firewall security level" on page 134.
Monitor firewall protection	Regularly check the firewall protection status on your computers. See "About monitoring endpoint protection" on page 69.

How the firewall works

Firewall protection prevents unauthorized users from accessing your computers and networks that connect to the Internet.

The packets of data that travel across the Internet contain information about the following:

- Sending computers
- Intended recipients
- How the packet data is processed
- Ports that receive the packets

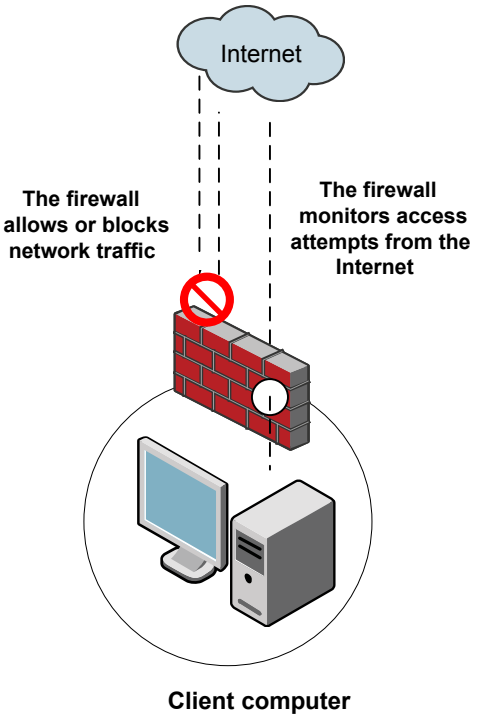
A packet is a discrete chunk of data that is part of the information flow between two computers. Packets are reassembled at their destination to appear as an unbroken data stream.

The ports are the channels that divide the stream of data that comes from the Internet. The applications that run on a computer listen to the ports. The applications accept the data that is sent to the ports.

Network attacks exploit weaknesses in vulnerable applications. Attackers use these weaknesses to send the packets that contain malicious programming code to ports. When vulnerable applications listen to the ports, the malicious code lets the attackers gain access to the computer.

Firewall protection works in the background. Firewall protection monitors the communication between your computers and other computers on the Internet. It creates a shield that allows or blocks attempts to access the information on your computers. It warns you of connection attempts from other computers. It warns

you of connection attempts by the applications on your computer that connect to other computers.



Firewall protection uses firewall rules to allow or block network traffic.

See "How the firewall rules work" on page 129.

Firewall protection supports the firewall rules that are written for specific ports and applications, and uses stateful inspection of all network traffic.

See "About firewall rules and stateful inspection" on page 132.

You enable default or custom firewall protection.

See "Enabling firewall protection" on page 134.

How the firewall rules work

Firewall rules control how the client protects your computers from malicious network traffic.

See "About the default firewall protection" on page 133.

When a computer attempts to connect to another computer, the firewall compares the connection type with the firewall rules. The firewall automatically checks all the inbound traffic packets and outbound traffic packets against the rules. The firewall allows or blocks the packets according to the rules.

Firewall rules are processed sequentially, from highest to lowest priority (from top to bottom in the rules list). If the first rule does not specify how to handle a packet, the firewall inspects the second rule. This process continues until the firewall finds a match. When the firewall finds a match, it takes the action that is specified in the rule. Subsequent lower priority rules are not inspected.

You can order rules according to exclusivity. The most restrictive rules are evaluated first, and the most general rules are evaluated last. For example, you should place the rules that block traffic near the top of the rules list. The rules that are lower in the list might allow the traffic.

You can use triggers such as applications, hosts, and protocols to define complex rules. For example, a rule can identify a protocol in relation to a destination address. When the firewall evaluates the rule, all the triggers must be true for a positive match to occur. If any trigger is false for the current packet, the firewall does not apply the rule.

You can enable and disable firewall rules. The firewall does not inspect disabled rules.

Table 14-2 lists the rule parameters that describe the conditions in which a network connection is allowed or blocked.

Table 14-2 Firewall rule parameters

Parameter	Description
Name	The name of the firewall rule.
Action	This parameter specifies what actions the firewall takes when it successfully matches a rule. The actions are as follows: ■ Allow The firewall allows the network connection. ■ Block The firewall blocks the network connection.

Table 14-2 Firewall rule parameters *(continued)*

Parameter	Description
Application	The applications that trigger the rule. When an application is the only trigger in an allow traffic rule, the firewall allows the application to perform any network operation. The application is the significant value, not the network operation that the application performs. For example, suppose you allow Internet Explorer, and define no other triggers. Computer users can access the remote sites that use HTTP, HTTPS, FTP, Gopher, and any other protocol that the Web browser supports. You can define additional triggers to describe the network protocols and hosts with which communication is allowed.
Host	The hosts that trigger the rule. You can define the host relationship as follows: ■ Local and remote hosts This relationship is commonly used in host-based firewalls. It is independent of the traffic direction. The local host is the local client computer. The remote host is the computer that communicates with the client computer. If the client communicates with a Web server, the remote host is the Web server and the local host is the client. The local host is the same for inbound traffic and outbound traffic. ■ Source and destination hosts This relationship is commonly used in network-based firewalls. It is dependent on the traffic direction. The source host is the computer that sends the packet. The source host is the remote computer for inbound traffic. The source host is the local computer for outbound traffic. The destination host is the computer that receives the packet. The destination host is the local computer for inbound traffic. The destination host is the remote computer for outbound traffic. If the client communicates with a Web server, and the traffic is inbound, the source host is the Web server and the destination host is the client. For outbound traffic, the source host is the client and the destination host is the Web server.

Table 14-2 Firewall rule parameters *(continued)*

Parameter	Description
Service	The network services that trigger a rule. A network service is a collection of the protocols and the port numbers that are grouped under one name. The network services list contains commonly used network services. For example, HTTP Server is the name for the HTTP server traffic that uses TCP local ports 80 and 443. DHCP Server is the name for the DHCP server traffic that uses UDP ports 67 and 68. When you define TCP or UDP service triggers, you identify the ports on both sides of the network connection. The port relationship is independent of the traffic direction. The local computer owns the local port. The remote computer owns the remote port.
Log	This parameter specifies whether Symantec Protection Center records successful and unsuccessful network connection attempts. The choices are as follows: ■ Yes The server records the network connection. ■ No The server does not record the network connection. ■ Send Email Alert An email notification is sent. You must configure the notification. See "Creating a notification" on page 98.

About firewall rules and stateful inspection

Firewall protection uses stateful inspection to track current connections. Stateful inspection tracks source and destination IP addresses, ports, applications, and other connection information. Before the client inspects the firewall rules, it makes the traffic flow decisions that are based on the connection information.

For example, if a firewall rule allows a computer to connect to a Web server, the firewall logs the connection information. When the server replies, the firewall discovers that a response from the Web server to the computer is expected. It permits the Web server traffic to flow to the initiating computer without inspecting the rule base. A rule must permit the initial outbound traffic before the firewall logs the connection.

Stateful inspection simplifies rule bases. For the traffic that is initiated in one direction, you do not have to create the rules that permit the traffic in both directions. The client traffic that is initiated in one direction includes Telnet (port

23), HTTP (port 80), and HTTPS (port 443). The client computers initiate this outbound traffic; you create a rule that permits the outbound traffic for these protocols. Stateful inspection automatically permits the return traffic that responds to the outbound traffic.

Stateful inspection supports all rules that direct TCP traffic.

Stateful inspection does not support the rules that filter ICMP traffic. For ICMP traffic, you must create the rules that permit the traffic in both directions. For example, for the clients to use the ping command and receive replies, you must create a rule that permits ICMP traffic in both directions.

About the firewall security levels

Firewall protection provides three levels of security.

Table 14-3 Firewall security levels

Security level	Description
Low	The Low security level allows all IP incoming traffic and outgoing traffic. Low is the default security level. See "About the default firewall protection" on page 133.
Medium	The Medium security level enforces the Low security level. It also blocks TCP incoming traffic and UDP stateful incoming traffic.
High	The High security level blocks all IP incoming traffic and outgoing traffic.

About the default firewall protection

The default firewall protection settings are defined in the Firewall Policy. By default, firewall protection is disabled in the policy.

When you enable firewall protection, the Symantec Firewall Policy allows all inbound and outbound IP-based network traffic, with the following exceptions:

- The default firewall protection blocks inbound and outbound IPv6 traffic with all remote systems.
- The default firewall protection restricts the inbound connections for a few protocols that are often used in attacks (for example, Windows File Sharing). Connections from the computers on internal networks are allowed. Connections from the computers on external networks are blocked.

The internal networks include the following IP ranges:

- 10.0.0.0/24

- 172.16.0.0/16
- 169.254.0.0/16
- 192.168.0.0/16

Table 14-4 lists the default Symantec Firewall Policy settings.

Table 14-4 Default Firewall Policy settings

Setting	Description
Enable this Firewall Policy	Check this box to enable the default firewall protection.
Security level	Low
Display notification on the computer when the client blocks an application	Disabled

Enabling firewall protection

You can enable the default firewall protection or the custom firewall protection.

To enable the default firewall protection

1. In the console, click **Policies**.
2. On the Policies page, select the Firewall Policy, and then right-click **Edit**.
3. In the policy, click **Firewall Rules**.
4. In the policy, check **Enable this Firewall Policy**.
5. Click **OK**.

To enable custom firewall protection

1. In the console, click **Policies**.
2. On the Policies page, select the Firewall Policy, and then right-click **Edit**.
3. In the policy, click **Firewall Rules**.
4. In the policy, check **Enable this Firewall Policy**.
5. In the policy, click **Customize the default settings**.
6. Click **OK**.

Adjusting the firewall security level

Adjusting the firewall security level restricts network traffic.

See "About the firewall security levels" on page 133.

To adjust the security level

1. In the console, click **Policies**.
2. On the Policies page, select the Firewall Policy, and then right-click **Edit**.
3. In the policy, click **Firewall Rules**.
4. In the policy, check **Enable this Firewall Policy**, and then select **Customize the default settings**.
5. In the policy, select the security level setting.
6. Click **OK**.

Configuring a firewall notification

You can alert computer users about a blocked application. A notification appears on the users' computers.

To configure a firewall notification

1. In the console, click **Policies**.
2. On the Policies page, select the Symantec Firewall Policy, and then right-click **Edit**.
3. Enable custom firewall protection.

   See "Enabling firewall protection" on page 134.
4. In the policy, on the Notifications tab, check the following options:

Display notification on the computer when the client blocks an application	A notification appears when the client blocks an application.
Add additional text to notification	Click **Set Additional Text** to customize the notification.

About adjusting firewall protection

You can increase firewall protection by adjusting the security level and modifying the firewall rules.

Table 14-5 Firewall protection adjustments

Setting	Description
Default or custom	Changing from default to custom lets you modify the security level and the firewall rules. See "Enabling firewall protection" on page 134.
Firewall rules	You can modify the default firewall rules. You can create new rules. Adjusting the firewall rules requires advanced knowledge of firewalls and firewall rules. Click Help for instructions on configuring the firewall rules.

Chapter 15

Managing intrusion prevention protection

This chapter includes the following topics:

About managing Intrusion Prevention protection

You manage Intrusion Prevention protection on the Policies page.

Table 15-1 Intrusion Prevention management

Task	Description
Learn about Intrusion Prevention	Learn how Intrusion Prevention detects and blocks network attacks. See "How Intrusion Prevention protection works" on page 138.
Review default settings	Review the default Intrusion Prevention settings. See "About the default Intrusion Prevention settings" on page 139.

Table 15-1 Intrusion Prevention management *(continued)*

Task	Description
Monitor Intrusion Prevention protection	Regularly check that Intrusion Prevention is enabled on your computers. See "About monitoring endpoint protection" on page 69.
Specify signature exceptions	Specify the signatures that have different detection responses. See "Specifying Intrusion Prevention exceptions" on page 140.

How Intrusion Prevention protection works

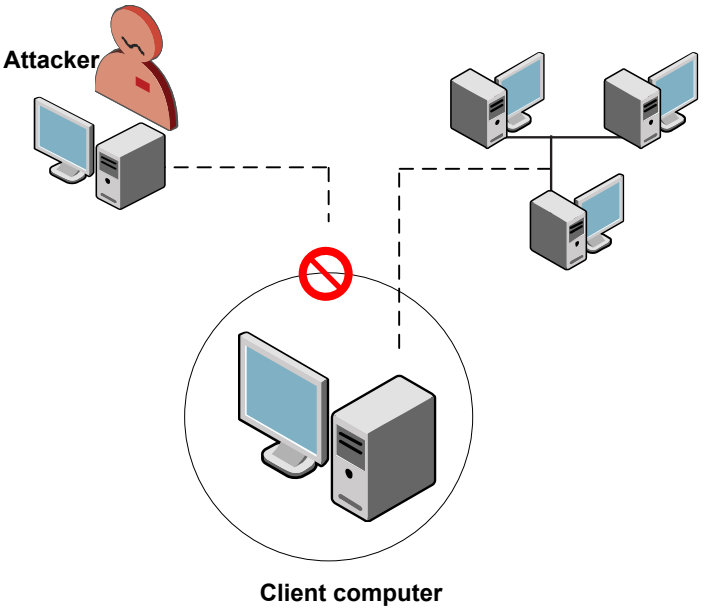
Intrusion Prevention protection automatically detects and blocks network attacks. Intrusion Prevention protection scans every packet that enters and exits a computer for attack signatures. An attack signature is a unique arrangement of information that identifies an attacker's attempt to exploit a known operating system or program vulnerability.

Intrusion Prevention protection uses Symantec's extensive list of attack signatures.

http://securityresponse.symantec.com/avcenter/attack_sigs/index.html

Intrusion Prevention protection optionally blocks all communication to and from an attacking computer for a specified period of time.

Figure 15-1 Intrusion Prevention protection



About the default Intrusion Prevention settings

The Intrusion Prevention Policy defines the default Intrusion Prevention settings.

Table 15-2 Default Intrusion Prevention settings

Setting	Description
Enable Intrusion Prevention	Enabled
Automatically block an attacker's IP address	Enabled Intrusion Prevention protection blocks an attacker's IP address for 600 seconds.
Exceptions	None

Enabling Intrusion Prevention

Intrusion Prevention automatically detects and blocks network attacks.

To enable Intrusion Prevention

1. In the console, click **Policies**.
2. On the Policies page, select the Intrusion Prevention Policy, and then right-click **Edit**.
3. In the policy, click **Settings**.
4. In the policy, click **Enable Intrusion Prevention**.
5. Click **OK**.

Blocking an attacking computer

Intrusion Prevention protection automatically blocks all communication to and from an attacking computer for a specified period of time. Intrusion prevention attacks are recorded in the Network Threat Protection Log.

See "Viewing the Network Threat Protection Log" on page 76.

To block an attacking computer

1. In the console, click **Policies**.
2. On the Policies page, select the Intrusion Prevention Policy, and then right-click **Edit**.
3. In the policy, click **Settings**.
4. In the policy, specify the following information:

Automatically block an attacker's IP address	Check this box to block all communication to and from an attacking computer.
Number of seconds during which to block the IP address	Type the number of seconds to block all communication to and from an attacking computer.

5. Click **OK**.

Specifying Intrusion Prevention exceptions

You specify the signatures that have different detection responses.

To specify Intrusion Prevention exceptions

1. In the console, click **Policies**.
2. On the Policies page, select the Intrusion Prevention Policy, and then right-click **Edit**.
3. In the policy, click **Exceptions**.
4. In the policy, click **Add**.
5. In the Add Intrusion Prevention Exceptions dialog box, select an exception, and then click **Next**.
6. In the Signature Action dialog box, specify the following options.

Action	You select one of the following actions: ■ Block ■ Allow
Log	You select one of the following log actions: ■ Log the traffic ■ Do not log the traffic

7. Click **OK**.

Chapter 16

Managing administrator accounts

This chapter includes the following topics:

About managing administrator accounts

You manage administrator accounts on the Admin page.

Table 16-1 Account administration

Task	Description
Decide who needs an account	Decide who needs to access Symantec Protection Center. Decide whether the access should be restricted or unrestricted. See "About administrator accounts" on page 144.
Create accounts	Create an account for the administrators and the users who need access to Symantec Protection Center. See "Creating an administrator account" on page 145.

Table 16-1 Account administration *(continued)*

Task	Description
Enable forgotten passwords	You can allow the administrators and the users to reset forgotten passwords. See "Enabling forgotten passwords" on page 145.

About administrator accounts

Administrator accounts provide secure access to the Symantec Protection Center console.

Roles are assigned to the administrator accounts. A role determines which functions an administrator can perform in the console.

Table 16-2 Administrator account roles

Role	Description
System administrator	Administrators with the System Administrator role can log on to the Symantec Protection Center console with complete, unrestricted access to all features and tasks.
Limited administrator	Administrators with the Limited Administrator role can log on to the Symantec Protection Center console with restricted access. An administrator with the System Administrator role determines the restrictions. Restrictions can affect the following items: ■ Reports You can limit an administrator's access to specific client computers. ■ Groups You can limit an administrator's access to specific groups. ■ Running commands on client computers You can limit an administrator's access to specific commands. ■ Policies You can limit an administrator's access to specific policies. ■ Licenses The Limited Administrator role does not have access to license information, including reports and notifications.

Creating an administrator account

You can create an account for administrators and users who need to access the Symantec Protection Center console.

To create an administrator account

1. In the console, click **Admin**.
2. On the Admin page, under Tasks, click **Add Administrator**.
3. In the Add Administrator dialog box, specify the account information.

   Click **Help** for more information.
4. Click **OK**.

Editing an administrator account

You can change the user name, password, and email address for an administrator account. Passwords must comprise at least six characters.

To edit an administrator account

1. In the console, click **Admin**.
2. On the Admin page, under Administrators , click an administrator user name, and then click **Edit the administrator**.
3. In the Edit System Administrator Properties dialog box, edit the account information.
4. Click **OK**.

Enabling forgotten passwords

You can allow administrators to reset forgotten passwords.

To enable forgotten passwords

1. In the console, click **Admin**.
2. On the Admin page, click **System**.
3. On the Admin page, click **Edit Properties**.
4. In the Server Properties dialog box, on the Security tab, check **Allow new passwords to be created for forgotten administrator passwords**.

   Uncheck the check box to disable forgotten passwords.
5. Click **OK**.

Chapter 17

Managing disaster recovery

This chapter includes the following topics:

Managing disaster recovery

Disaster recovery restores Symantec Protection Center and allows it to resume communicating with the client computers.

You can use disaster recovery in the following situations:

- You want to reinstall the server because the database is damaged.
- You want to move the server installation to another computer because the old computer's hard disk is damaged.
- You want to move the server installation to a new computer.

Table 17-1 Disaster recovery steps

Step	Action	Description
Step 1	Prepare for disaster recovery	You must prepare for the possibility that you might need to use disaster recovery. See "About preparing for disaster recovery" on page 148.

Table 17-1 Disaster recovery steps *(continued)*

Step	Action	Description
Step 2	Recover the server	Recovering the server reinstalls the server software and allows it to resume communicating with client computers. Select one of the following server recovery methods: ■ Uninstall and then reinstall Symantec Protection Center on the same computer. See "Reinstalling Symantec Protection Center" on page 150. ■ Move Symantec Protection Center to a computer that does not currently run the server software. See "Moving the server" on page 149. **Note:** Recovering the server does not restore the database.
Step 3	Restore the database	The database contains security policies, license files, events, groups, and other data. This step is optional. See "Restoring the database" on page 151.

About preparing for disaster recovery

You must prepare for the possibility that you might need to use disaster recovery.

Table 17-2 Disaster recovery preparation

Task	Description
Back up the Server Private Key Backup folder	After you install or reinstall the server, back up the Server Private Key Backup folder that is stored on the Symantec Protection Center computer. The Server Private Key Backup folder contains the data recovery file, which the server uses to communicate with the client computers. By default, the Server Private Key Backup folder is located in the following directory: C:\Program Files\Symantec\Symantec Protection Center Copy the Server Private Key Backup folder and its contents to another computer of your choice.
Back up license files	Backing up the license files preserves the files in case the database or the computer's hard disk is damaged. See "Backing up your license files" on page 109.

Table 17-2 Disaster recovery preparation *(continued)*

Task	Description
Back up database	Back up the database at least weekly. The database stores important data such as security policies, events, and groups. See "Backing up the database" on page 149.

Backing up the database

Symantec recommends that you back up the database at least weekly. You should store the backup file on another computer.

Note: Avoid saving the backup file in the product installation directory. Otherwise, the backup file is removed when the product is uninstalled. The default installation directory is C:\Program Files\Symantec\Symantec Protection Center.

The database backup might take several minutes to complete.

To back up the database

1. On the computer that runs Symantec Protection Center, on the Start menu, click **All Programs > Symantec Protection Center > Symantec Protection Center Tools > Database Back Up and Restore**.
2. In the Database Back Up and Restore dialog box, click **Back Up**.
3. Click **Yes**.
4. Click **OK**.
5. When the database backup completes, click **Exit**.
6. Copy the backup database file to another computer of your choice.

   By default, the backup database file is named *date_timestamp*.zip. The file is saved in the following directory:

   C:\Program Files\Symantec\Symantec Protection Center\data\backup

Moving the server

This disaster recovery method moves Symantec Protection Center to a computer that does not run Symantec Protection Center.

Disaster recovery requires that you have a backup of the Server Private Key Backup folder.

See "About preparing for disaster recovery" on page 148.

To move the server

1. On the computer where you want to move Symantec Protection Center, create the following directory:

   C:\Program Files\Symantec\Symantec Protection Center

2. Copy your backup of the Server Private Key Backup folder and its contents to the directory.

3. Install the server software.

   When you install the server, you are asked if you want to load the disaster recovery data file.

   See "Installing the server and the console" on page 35.

4. If you do not restore the database, log on to the console, and then import your license files.

   See "Importing a license" on page 107.

   If you restore the database, the license files are restored with the database.

   See "Restoring the database" on page 151.

Reinstalling Symantec Protection Center

This disaster recovery method uninstalls Symantec Protection Center. It reinstalls the software on the same computer, in the same installation directory.

Disaster recovery requires that you have a backup of the Server Private Key Backup folder.

See "About preparing for disaster recovery" on page 148.

To reinstall Symantec Protection Center

1. On the server computer, uninstall the server software.

   See "Uninstalling Symantec Protection Center" on page 39.

2. Make sure the Server Private Key Backup folder exists on the computer.

   By default, the Server Private Key Backup folder is saved in the following directory:

   C:\Program Files\Symantec\Symantec Protection Center

   If the Server Private Key Backup folder does not exist, copy your backup of the folder to the directory.

3 Install the server software.

See “Installing the server and the console” on page 35.

4 If you do not restore the database, log on to the console, and then import your license files.

See “Importing a license” on page 107.

If you restore the database, the license files are restored with the database.

See “Restoring the database” on page 151.

Restoring the database

You must restore the database using the same version of Symantec Protection Center that you used to back up the database. The database restore might take several minutes to complete.

You can restore the database on the same computer on which it was installed originally. You can install the database on a different computer.

Review the instructions before you restore the database.

To restore the database on the same computer

1 On the computer that runs Symantec Protection Center, on the Start menu, click **Settings > Control Panel > Administrative Tools > Services**.

2 In the Services window, click **Symantec Protection Center**, and then click **Stop**.

Do not close the Services window.

3 Create the following directory:

C:\Program Files\Symantec\Symantec Protection Center\data\backup

4 Copy the backup database file to the directory.

By default, the backup database file is named *date_timestamp*.zip.

5 On the Start menu, click **All Programs > Symantec Protection Center > Symantec Protection Center Tools > Database Back Up and Restore**.

6 In the Database Back Up and Restore dialog box, click **Restore**.

7 Click **Yes** to confirm the database restoration.

8 In the Restore Site dialog box, select the backup database file, and then click **OK**.

9 Click **OK**.

10 Click **Exit**.

11 In the Services window, click **Symantec Protection Center**, and then click **Start**.

12 Close the Services window.

13 On the Start menu, click **All Programs > Symantec Protection Center > Symantec Protection Center Console** to start the console.

The client computers connect to the server within 30 minutes.

To restore the database on a different computer

1 Follow steps 1-10 from the previous procedure.

2 Run the Server Configuration Wizard to verify and optionally modify the server installation settings.

See "Modifying the server installation settings" on page 156.

3 Follow the on-screen prompts to finish the database restoration.

4 Close the Services window.

Loading a disaster recovery file

The installation detected a disaster recovery data file from a previous server installation. The disaster recovery data file is used to restore communication between the server and the client computers.

Click Help for more information about disaster recovery.

See "Managing disaster recovery" on page 147.

To load a disaster recovery data file

1 Click **Yes** to load the disaster recovery data file.

Click **No** to skip loading the disaster recovery data file. The server does not resume communicating with the client computers.

2 Click **OK**.

Appendix A

Maintaining and troubleshooting Symantec Endpoint Protection Small Business Edition

This appendix includes the following topics:

Restarting client computers

You can restart a selected computer. You can restart all the client computers in a selected group.

To restart a selected client computer

1. In the console, click **Computers**.
2. On the Computers page, on the Computers tab, select a group.
3. On the Computers tab, select a computer, right-click **Run Command on Group**, and then click **Restart Client Computers**.

To restart the client computers in a selected group

1. In the console, click **Computers**.
2. On the Computers page, on the Computers tab, select a group, right-click **Run Command on Group**, and then click **Restart Client Computers**.

Finding managed computers

You can search for managed computers by group.

To find managed computers

1. In the console, click **Computers**.
2. On the Computers page, on the Computers tab, click **Search for computers**.
3. In the Search for Computers dialog box, select the group.
4. In the Search for Computers dialog box, specify the search criteria.

   Click **Help** for more information about the search criteria.
5. Click **Search**.

   To search for unmanaged computers, use the network search function in the Remote Push Installation. Once you find the unmanaged computer, you can cancel the installation.

   See "Deploying clients by using Remote Push Installation" on page 50.

Converting an unmanaged computer

You or the computer user can convert an unmanaged computer to a managed computer.

See "About managed and unmanaged computers" on page 46.

You can convert an unmanaged computer to a managed computer by using the following methods:

- Install the client as a managed computer.

This method converts an unmanaged computer to a managed computer by reinstalling the client software.
See "Installing the Symantec Endpoint Protection Small Business Edition client" on page 45.

- Import the server communications settings.
  This method converts an unmanaged computer to a managed computer by importing the server communications settings.

Table A-1 lists the steps to import the server communications settings.

Table A-1 Server communication settings import steps

Step	Task	Description
Step 1	Provide server communications settings to computer user	Export the sylink.xml file that contains the server communication settings for a group. Do the following tasks to export the sylink.xml file: ■ In the console, on the Computers page, select a group, and then right-click Export Communications Settings. ■ Follow the prompts to save the sylink.xml file. Do not edit the file. ■ Email the sylink.xml file to the computer user, or save the file to a user-shared location.
Step 2	Import sylink.xml	Import the sylink.xml file into the client computer. Do the following tasks to import the sylink.xml file: ■ On the unmanaged client computer, open the client. ■ Click Help, and then click Troubleshooting. ■ In the Management dialog box, under Communication Settings, click Import. ■ Follow the prompts to locate the sylink.xml file. The client computer immediately connects to the server. The server places the computer in the group. The computer is updated with the group's security policies and settings. After the computer communicates with the server, the notification area icon appears on the computer's desktop.
Step 3	Verify client and server communication	Verify that the computer communicates with the server. Do the following tasks to verify server communication: ■ In the console, on the Computers page, verify that the client computer is online. Verify that the computer is in the correct group; move the computer to the correct group if necessary. ■ On the computer, in the client, click Help, and then click Troubleshooting. The name of the server is listed under General Information.

Finding the server host name and IP address

You can locate the Symantec Protection Center server host name and IP address.

To find the server host name and IP address

1. In the console, click **Admin**.
2. On the Admin page, click **System**.

   The Server Name box shows the Symantec Protection Center server host name. The Address box shows the IP address.

Modifying email server settings

You can change the email server settings that were established during the server installation.

See "About the Symantec Protection Center installation settings" on page 33.

To modify email server settings

1. In the console, click **Admin**.
2. On the Admin page, under System, click **Edit Properties**.
3. In the Server Properties dialog box, on the Email Server tab, edit the email settings.

   Click Help for assistance.
4. Click **OK**.

Modifying the server installation settings

You might need to modify the Symantec Protection Center installation settings in the following situations:

- You restored the database on a different computer than it was installed originally.
- You want to modify a server setting or a database setting.

See "About the Symantec Protection Center installation settings" on page 33.

You run the Server Configuration Wizard to modify the Symantec Protection Center installation settings.

To modify the Symantec Protection Center installation settings

1. On the console computer, on the Start menu, click **All Programs > Symantec Protection Center > Symantec Protection Center Tools > Management Server Configuration Wizard**.
2. In the wizard, click **Reconfigure the management server**, and then click **Next**.
3. In the wizard, optionally modify the server settings and the database settings, and then click **Next** after each wizard panel.
4. Follow the onscreen prompts to finish the server configuration.

Investigating client problems

To investigate client problems, you can examine the Troubleshooting.txt file. The Troubleshooting.txt file contains information about policies, virus definitions, and other client-related data.

To investigate client problems

1. On the client computer, open the client.
2. In the client, click **Help**, and then click **Troubleshooting**.
3. In the client, under Troubleshooting Data, click **Export**.
4. In the Save As dialog box, accept the default troubleshooting file name or type a new file name, and then click **Save**.

   You can save the file on the desktop or in a folder of your choice.
5. Using a text editor, open Troubleshooting.txt to examine the contents.

   Contact Symantec Technical Support for assistance. Symantec Technical Support might request that you email the Troubleshooting.txt file.

Troubleshooting Symantec Protection Center communication problems

Instructions and suggestions to resolve Symantec Protection Center communication problems are available in the Symantec Knowledge Base article, Troubleshooting Symantec Protection Center communication problems.

Troubleshooting content update problems

Instructions and suggestions for troubleshooting content update problems are available in the Symantec Knowledge Base article, Troubleshooting content update problems.

Providing information for Symantec Support

You can gather detailed information for Symantec Support.

To provide information for Symantec Support

1. Run the Symantec Protection Center Support Tool.

   The Support Tool is available on the computer that hosts Symantec Protection Center. The Support Tool is also available on the client computers.

2. Click **Help > Download Support Tool**.

3. Follow the onscreen instructions.

Appendix B

Managing mobile clients and remote clients

This appendix includes the following topics:

About mobile clients and remote clients

Today's workforce is no longer tied to a single location, because employees increasingly work remotely or from multiple locations. This situation has created a type of client that is distinct from other clients in your network. A mobile client is defined as a client that moves physically from location to location. Employees who travel in the course of their job typically use these client computers. Such client computers connect to the network intermittently and are often in an unknown state. Their users typically log on through a virtual private network (VPN). Remote clients are defined as clients that always connect from the same location, but they are not physically located within the corporate network. Typical examples of remote clients are employees who work from their homes and logon through a VPN. Both types of clients are subject to similar risks and should be treated similarly.

Mobile clients and remote clients are more at risk than the clients that always reside within your corporate network. Mobile clients and remote clients are outside

the safety of your corporate defenses. The management of these clients places an extra burden on administrators to maintain the safety of the network and its data.

You might have mobile clients and remote clients in your network for a number of different reasons, and they might exhibit different patterns of usage. For example, you may have some internal computers that periodically move outside your corporate environment. You may have some sales personnel whose computers are never inside the network. You may have some client computers that need to connect to your network but are completely outside your administrative control. For example, you may allow customers, contractors, vendors, or business partners limited access to your network. You may have employees who connect to the corporate network using their own personal computers.

Some mobile users and remote users might have a less stringent attitude toward Internet browsing than you want, and therefore exhibit riskier behavior. The mobile users and remote users that do not work directly for your business may not be as educated about computer security as your employees. For example, they might be more likely to open email messages or attachments from unknown sources while on your network. They may be more likely to use weak passwords. Mobile users and remote users in general may be more likely to make unauthorized changes or to customize their computers. For example, they may be more likely to download and use an application that has not been approved for corporate use. Mobile users and remote users may be so focused on doing their work as quickly as possible that they fail to think about computer security.

Because it is a best practice to treat both remote clients and mobile clients similarly, we refer to both types of clients as remote clients.

About setting up groups for remote clients

The number of groups you need depends on two main factors: the types of remote clients you have and the security restrictions you want to apply to each type of client. The types of remote clients you create separate groups for may include the following:

- Employees that log on to your network through a virtual private network (VPN).
- Employees that log on to your network without using a VPN.
- Users that are not employees of your company but who need access to your network.

After you determine the types of remote clients that you have, you should consider what security restrictions to apply to each of them. You control security restrictions with policies. Each type of protection is controlled with its own policy.

For example, virus and spyware, firewall, LiveUpdate, and intrusion protection each have a separate policy. Only one policy for each type of protection can be applied to any given group. Therefore, to establish more than one level of restrictions, separate groups must be created and then assigned the appropriate protection policies.

The fewer the number of groups that you create, the simpler it is to manage your security policies.

For information about how to set up groups and policies, see the *Implementation Guide for Symantec Endpoint Protection Small Business Edition*.

As a best practice, you should not allow users to turn off the following protections:

- Auto-Protect
- TruScan proactive threat scans
- The firewall rules that you have created

About strengthening your security policies for remote clients

When you manage remote users, you essentially take some form of one of the following positions:

- Leave the default policies in place, so that you do not impede remote users in the use of their computers.
- Strengthen your default security policies to provide more protection for your network, even if it restricts what remote users can do.

In most situations, the best practice is to strengthen your security policies for remote clients.

About best practices for Firewall Policy settings

A best practice for a Firewall Policy is to assign the strictest security policies to clients that log on remotely without using a VPN. In addition to the default settings, to increase security, you can block all local TCP traffic on the NetBios ports 135, 139, and 445.

The following settings are recommended as best practice for the Firewall Policy for the remote clients where users log on through a VPN:

- Leave as-is all the rules that block traffic from any Host.
- Leave as-is the rule that allows VPN traffic from any Host.

- Leave as-is the rule that blocks all other traffic.

As a best practice for the Firewall policies for the groups where users log on through Ethernet or wireless connections, use your default Firewall Policy. For the wireless connection, ensure that the rule to allow wireless EAPOL is enabled. 802.1x uses the Extensible Authentication Protocol over LAN (EAPOL) for connection authentication.

About best practices for Virus and Spyware Policy settings

As a best practice for the Virus and Spyware policies for remote clients, use your default Virus and Spyware Policy. The default policy suspends scans when the remote client operates from batteries to extend battery life.

About best practices for LiveUpdate Policy settings

If you maintain strict control over Symantec content and product updates for your clients, you should consider changing your LiveUpdate Policy for your remote clients.

For the group of remote users who log on without a VPN, we suggest you change the LiveUpdate Scheduling frequency to one hour. This setting makes it more likely that clients update their protection when they connect to the Internet.

For all other groups, it is a best practice to use the Symantec Protection Center to distribute product software and content updates. An update package that is distributed through the management console is incremental rather than a complete package. The update packages are smaller than the packages that are downloaded directly from the Symantec LiveUpdate server.

About client notifications

For your remote clients that are not logged on over VPN, it is a best practice to turn on notifications for virus and security risks. You can turn on these notifications in the Virus and Spyware policy.

Turning on notifications helps to ensure that remote users are aware when a security problem occurs.

About monitoring remote clients

Notifications and logs are essential to maintain a secure environment. In general, you should monitor your remote clients in the same way that you monitor your other clients. You should always check to see that your protections are up to date

and that your network is not currently under attack. If your network is under attack, then you want to find out who is behind the attack and how they attacked.

You can check the following displays to monitor the security of your environment:

Home > Endpoint Status	You can check the following status conditions: ■ Content dates and version numbers ■ Client connections ■ Enabled and disabled protections You can click Details to see the status for each client.
Home > Security Status	System security overview You can click Details to see the status for each security protection technology.
Home > Virus and Risks Activity Summary	Network attack activity
Monitors > Summary Type	You can select Network Threat Protection to see information about attack types and sources.

The data on the Home page in the following displays represents only the clients that connected in the past 12 hours or 24 hours:

- Virus Definitions Distribution
- Intrusion Prevention Signatures
- Status Summary

Your Home page preference settings determine the time period for which Symantec Protection Center displays data. If you have many clients that are frequently offline, your best monitoring option is to go to the logs and reports. In the logs and reports, you can filter the data to include offline clients.

Index

P

R

S

T

V