Administration Guide for Symantec™ Endpoint Protection and Symantec Network Access Control

Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control

Documentation version 11.00.06.00.00

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

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 support 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/or web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

www.symantec.com/business/support/

Contacting Technical Support

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

www.symantec.com/business/support/

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/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as 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 support 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

Support agreement resources

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

Asia-Pacific and Japan	customercare_apac@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:

Managed Services	Managed 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.
Education Services	Education 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/business/services/

Select your country or language from the site index.

Contents

Section 1

Basic administrative tasks

Chapter 1

Introducing Symantec Endpoint Protection

This chapter includes the following topics:

About Symantec Endpoint Protection

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

See "About the types of protection" on page 33.

Symantec Endpoint Protection protects against malware such as viruses, worms, Trojan horses, spyware, and adware. It provides protection against even the most sophisticated attacks that evade traditional security measures such as rootkits, zero-day attacks, and spyware that mutates. Symantec Endpoint Protection also lets you maintain fine-grained application and device control. Symantec Endpoint Protection provides multiple layers of protection for your endpoint computing devices.

Your Symantec software may include Symantec Network Access Control. Symantec Network Access Control also uses Symantec Endpoint Protection Manager to install and manage Symantec Endpoint Protection clients and Symantec Network Access Control clients. Symantec Network Access Control ensures that clients are compliant with your organization's security policies before they are allowed access to your network. Symantec Endpoint Protection and Symantec Network Access Control work together but are purchased separately.

See "About Symantec Network Access Control" on page 28.

See "Components of Symantec Endpoint Protection and Symantec Network Access Control" on page 28.

About Symantec Network Access Control

Symantec Network Access Control ensures that a company's client computers are compliant with the company's security policies before the computers are allowed to access the network. Symantec Network Access Control uses a Host Integrity Policy and an optional Symantec Enforcer to discover and evaluate which computers are compliant. The clients that are not compliant are directed to a remediation server. The remediation server downloads the necessary software, patches, virus definitions updates, and so on, to make the client computer compliant. Symantec Network Access Control also continually monitors endpoints for changes in the compliance status.

Symantec Network Access Control is a companion product to Symantec Endpoint Protection. Both products include Symantec Endpoint Protection Manager, which provides the infrastructure to install and manage the Symantec Endpoint Protection and Symantec Network Access Control clients. The Symantec Endpoint Protection client protects your endpoints from both known threats and those threats that have not been seen before.

See "About Symantec Endpoint Protection" on page 27.

See "Components of Symantec Endpoint Protection and Symantec Network Access Control" on page 28.

For more information about the Enforcer appliance, see the *Implementation Guide for Symantec Network Access Control Enforcement*.

Components of Symantec Endpoint Protection and Symantec Network Access Control

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

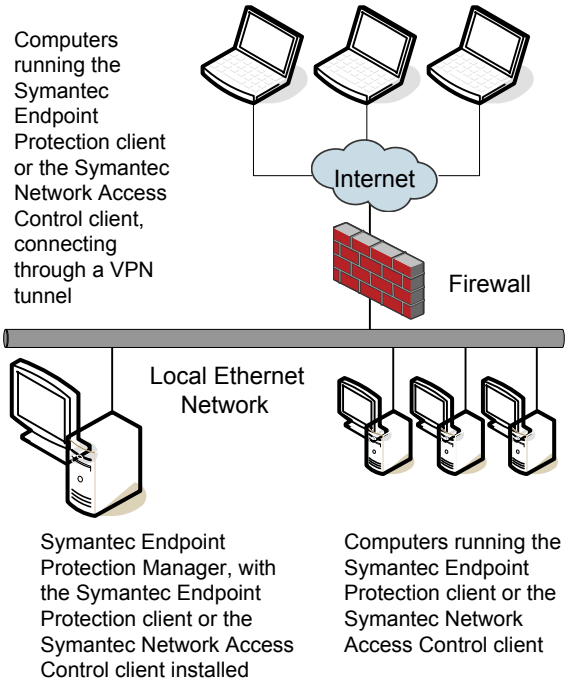
Table 1-1 Product components

Component	Description
Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager is a management server that manages the client computers that connect to your company's network. Symantec Endpoint Protection Manager includes the following software: ■ The console software coordinates and manages security policies and client computers. ■ The server software provides secure communication to and from the client computers and the console. See "What you can do from the console" on page 40.
Database	The database that stores security policies and events. The database is installed on the computer that hosts Symantec Endpoint Protection Manager. See "About the management of databases" on page 343.
Symantec Endpoint Protection client	The Symantec Endpoint Protection client protects the computers with virus scans, a firewall, an intrusion prevention system, and other protection technologies. It runs on the servers, desktops, and portable computers that you want to protect. For more information, see the *Client Guide for Symantec Endpoint Protection and Symantec Network Access Control.*
Symantec Network Access Control client	The Symantec Network Access Control client enforces security policy compliance on the client computers by using Host Integrity checks and self-enforcement capabilities. The client reports its Host Integrity compliance status to a Symantec Enforcer. For more information, see the *Implementation Guide for Symantec Network Access Control Enforcement.* For more information, see the *Client Guide for Symantec Endpoint Protection and Symantec Network Access Control.*
Symantec Protection Center	Symantec Protection Center is installed when you install Symantec Endpoint Protection Manager. Protection Center lets you integrate management consoles from multiple supported Symantec security products into a single management environment. See "About Symantec Protection Center" on page 43.

Table 1-1 Product components *(continued)*

Component	Description
Symantec Enforcer (optional)	An Enforcer ensures that the clients that try to connect to the network comply with configured security policies. You can restrict non-compliant computers to specific network segments for remediation and you can completely prohibit access to non-compliant computers. Symantec Network Access Control includes the following types of Enforcers: ■ The Enforcer appliance, which is a hardware appliance on which you install one of several Symantec Enforcer appliance images. ■ The Integrated Enforcers, which are the software components that interact with a Microsoft DHCP Server and a Microsoft Windows Network Policy Server. For more information, see the *Implementation Guide for Symantec Network Access Control Enforcement*.
Symantec Network Access Control On-Demand clients for Windows and Macintosh (optional)	On-Demand clients are the temporary clients that you provide to users when they are unauthorized to access your network because they do not have the software that is compliant with your security policy.
LiveUpdate Server (optional)	The LiveUpdate Server downloads definitions, signatures, and product updates from a Symantec LiveUpdate server and distributes the updates to client computers. For more information, see the *Symantec LiveUpdate Administrator User's Guide*.
Central Quarantine (optional)	The Central Quarantine receives suspicious files and unrepaired infected items from the Symantec Endpoint Protection clients. Central Quarantine forwards a sample to Symantec Security Response, which analyzes the sample. If a threat is new, Symantec Security Response produces security updates. For more information, see the *Symantec Central Quarantine Implementation Guide*.

Figure 1-1 The product components in a network



See "About Symantec Endpoint Protection" on page 27.

See "About Symantec Network Access Control" on page 28.

See "Key features of Symantec Endpoint Protection and Symantec Network Access Control" on page 32.

Key features of Symantec Endpoint Protection and Symantec Network Access Control

Table 1-2 Product key features

Feature	Description
Enterprise-level protection	The product provides the following features: ■ Client computer scans for viruses and security threats. ■ Detection and repair of the effects of known viruses, worms, Trojan horses, spyware, adware, and rootkits. ■ Analysis of processes for behavior anomalies to detect known and unknown viruses and security risks. ■ Prevention of unauthorized users from accessing the computers and networks that connect to the Internet. ■ Cleaning, deleting, and quarantining infected files. ■ Automatic detection and blocking of network attacks. See "About the types of protection" on page 33.
Management	The following features are included: ■ Out-of-the-box configuration for any size business. ■ Symantec Protection Center console optionally lets you integrate more than one Symantec product management console into a single environment. See "About Symantec Protection Center" on page 43. ■ Single Symantec Endpoint Protection Manager console provides a view of the entire client deployment. See "What you can do from the console" on page 40. ■ Symantec Endpoint Protection Manager coordinates console and client communication and event logging. ■ Administrator accounts that provide access to the console. See "Managing domains and administrator accounts" on page 289. ■ LiveUpdate downloads of the latest virus definitions and product updates. See "Managing content for clients" on page 132.
Migration	The following features are included: ■ Group and policy settings from Symantec legacy software. ■ Client computer upgrades using the Client Installation Wizard.

Table 1-2 Product key features *(continued)*

Feature	Description
Client enforcement	The following features are included: ■ Ensures that a client computer is properly protected and compliant before it is allowed to connect to the corporate network. ■ Remediates the non-compliant client computers.

See "About Symantec Endpoint Protection" on page 27.

See "About Symantec Network Access Control" on page 28.

About the types of protection

Symantec Endpoint Protection enforces virus and other protection technologies on the client computers using several layers of essential protection.

Table 1-3 Symantec Endpoint Protection layers of protection

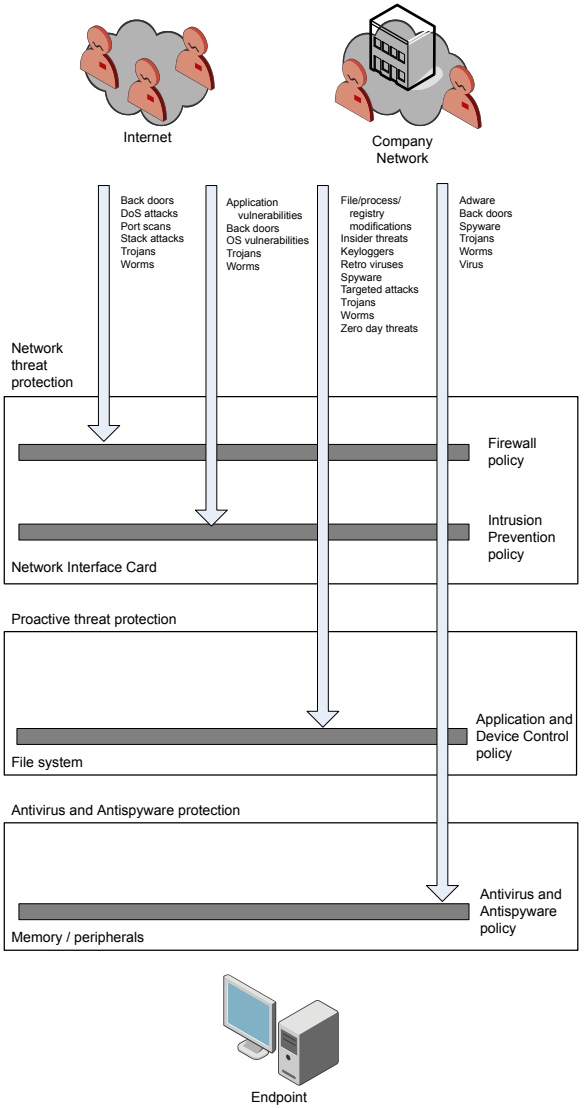
Protection type	Description
Antivirus and Antispyware Protection	Symantec Endpoint Protection Antivirus and Antispyware Protection provides protection from viruses and security risks, and in many cases can repair their side effects. The protection includes real-time scanning of files and email as well as scheduled scans and on-demand scans. Antivirus and antispyware scans detect both viruses and security risks, such as spyware, adware, and other files that can put a computer, as well as a network, at risk. See "Basics of Antivirus and Antispyware Protection" on page 386.

Table 1-3 Symantec Endpoint Protection layers of protection *(continued)*

Protection type	Description
Network Threat Protection	Network Threat Protection provides a firewall and intrusion prevention protection to prevent intrusion attacks and malicious content from reaching the computer that runs the Symantec Endpoint Protection client. The firewall allows or blocks network traffic based on various criteria that the administrator or end user sets. The client also analyzes all the incoming and the outgoing information for the data patterns that are typical of an attack. It detects and blocks malicious traffic and attempts by outside users to attack the client computer. Intrusion prevention also monitors outbound traffic and prevents the spread of worms. See "About Network Threat Protection and network attacks" on page 460.
Proactive Threat Protection	Proactive Threat Protection provides protection against zero-day attack vulnerabilities in your network. Zero-day attack vulnerabilities are new vulnerabilities that are not yet publicly known. Threats that exploit these vulnerabilities can evade signature-based detection (such as antispyware and antispyware definitions). Zero-day attacks may be used in targeted attacks and in the propagation of malicious code. Proactive Threat Protection includes the following: ■ TruScan proactive threat scans ■ Application and Device Control Policies See "About TruScan proactive threat scans" on page 519. See "About application and device control" on page 535.
Host Integrity	Host Integrity gives you the ability to define, enforce, and restore the security of clients to secure enterprise networks and data. You set up Host Integrity Policies to verify that clients attempting network access are running antivirus software, patches, and hotfixes and other application criteria. You set up Host Integrity Policies to run on client computers at startup and periodically afterward. **Note:** Host Integrity Policies are available only with the Symantec Network Access Control product. Symantec Network Access Control can be installed alone, or can be installed with Symantec Endpoint Protection. All other categories of protection are standard with Symantec Endpoint Protection, and do not come with Symantec Network Access Control.

Figure 1-2 shows the categories of threats that are blocked by each type of protection.

Figure 1-2 An overview of Symantec Endpoint Protection protection layers



Chapter 2

Starting the Symantec Endpoint Protection Manager console

This chapter includes the following topics:

Logging on to the Symantec Endpoint Protection Manager console

You can log on to the Symantec Endpoint Protection Manager console after you install Symantec Endpoint Protection. You can log on to the console in either of two ways:

- Locally, from the computer on which the management server is installed
- Remotely, from any computer that meets the system requirements for a remote console and has network connectivity to the management server.

Many administrators log on remotely, and they can do the same tasks as administrators who log on locally. To log on remotely, you need to know the IP address or the host name of the computer on which the management server is installed. You should also ensure that your Web browser Internet options allow you to view content from the server you log on to.

What you can view and do from the console depends on the type of administrator you are. You can log on as a system administrator, an administrator, or a limited administrator. A system administrator has full privileges across all domains. An

administrator has those privileges that are constrained to a specific domain. A limited administrator has a subset of the administrator privileges and is also constrained to a specific domain. If you installed the management server, you are a system administrator. If someone else installed the management server, your status may be different. Most organizations, however, do not need to be concerned about domains or limited administrator status.

You can also access the reporting functions from a stand-alone Web browser that is connected to your management server.

See "Logging on to reporting from a stand-alone Web browser" on page 194.

Most administrators in smaller organizations log on as a system administrator.

See "About administrators" on page 293.

Once you log on, you can access the Symantec Endpoint Protection Manager.

See "What you can do from the console" on page 40.

To log on to the console remotely

1 Open Internet Explorer and type the following address in the address box:

http://*host name*:9090

where *host name* is the host name or IP address of the management server.

Note: Internet Explorer 7 or higher is required to use the Symantec Endpoint Protection ManagerWeb Console

---

2 On the Symantec Endpoint Protection Manager console Web Access page, click the desired console type.

Note: If you select Symantec Endpoint Protection Manager Console, the computer from which you log on must have the Java 2 Runtime Environment (JRE) installed. If it does not, you are prompted to download and install it. Follow the prompts to install the JRE. The computer must also have Active X and scripting enabled.

---

3 When you log on, you may see a message that warns of a host name mismatch or a security warning. If the host name message appears, click **Yes**.

This message means that the remote console URL that you specified does not match the Symantec Endpoint Protection certificate name. This problem occurs if you log on and specify an IP address rather than the computer name of the management server.

If the Web page security certificate warning appears, click **Continue to this website (not recommended)** and add the self-signed certificate to Internet Explorer.

This message means that Internet Explorer does not recognize the linked site as being secure. Internet Explorer relies on security certificates to determine if a site is secure.

For instructions to add the security certificate to Internet Explorer, see the Symantec Technical Support Knowledge Base article, How to add the self-signed certificate for Symantec Protection Center or Symantec Endpoint Protection Manager to Internet Explorer.

4 Follow the prompts to complete the log on process. Depending on the log on method, you may need to provide additional information. For instance, if your network has multiple domains, you will need to provide the name of the domain you want to log on to.

Note: If this logon is the first logon after installation, use the account name, **admin**

---

5 Click **Log On**.

You may receive one or more security warning messages as the remote console starts up. If you do, click **Yes**, **Run**, **Start**, or their equivalent, and continue until the console appears.

To log on to the console locally

1 On the Windows Start menu, click **Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Console**.

2 In the Symantec Endpoint Protection Manager logon prompt, type the user name (admin by default) and password that you configured during the installation

If you are an administrator and you did not install the management server, use the user name and password that your administrator configured for you.

3 Do one of the following tasks:

- If the console has only one domain, skip to step 4.
- If the console has more than one domain, click **Options>>** and type the domain name.

4 Click **Log on**.

What you can do from the console

The Symantec Endpoint Protection Manager 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.

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

Table 2-1 Symantec Endpoint Protection Manager 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. ■ Adjust console preferences. ■ Get information about the latest Internet and security threats. See "About the Symantec Endpoint Protection Home page" on page 198. See "Using the Symantec Network Access Control Home page" on page 207.
Monitors	Monitor event logs that concern Symantec Endpoint Protection Manager 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. See "Monitoring endpoint protection" on page 191. See "Using the Monitors Summary tab" on page 208.

Table 2-1 Symantec Endpoint Protection Manager console pages *(continued)*

Page	Description
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. See "Creating quick reports" on page 250. See "Monitoring endpoint protection" on page 191.
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. See "Managing content for clients" on page 132. See "Using policies to manage your network security" on page 90.
Clients	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. See "Managing computer groups" on page 54.

Table 2-1 Symantec Endpoint Protection Manager console pages *(continued)*

Page	Description
Admin	Manages Symantec Endpoint Protection Manager 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. ■ Adjust the LiveUpdate schedule. ■ Download content updates from LiveUpdate. ■ View LiveUpdate status and recent downloads. See "Managing domains and administrator accounts" on page 289. See "Adding an administrator account" on page 296. See "Managing content for clients" on page 132.

Chapter 3

Managing the Symantec Endpoint Protection Manager console with Symantec Protection Center

This chapter includes the following topics:

About Symantec Protection Center

Symantec Protection Center is a Web-based console that lets you integrate management of your Symantec security products into a single environment. Protection Center includes a centralized Dashboard that reports on the overall security of your network based on the products that you integrate.

See "The Symantec Protection Center Dashboard" on page 46.

You integrate supported products in Protection Center in a registration process. After you register your products, you log on to Protection Center to manage them all.

The products must be installed and configured separately before you can register them. Registered, or integrated, products still function independently of Protection Center. You can manage the products together, in Protection Center, or separately, in the individual product consoles.

Integrated products are purchased separately or as part of a suite. Only Symantec Endpoint Protection includes Symantec Protection Center.

The following products can be integrated into Protection Center:

- Symantec Endpoint Protection
- Symantec Critical System Protection
- Symantec Web Gateway
- Symantec Brightmail Gateway
- Symantec Data Loss Prevention
- Symantec IT Analytics

The products and product versions that are supported by Symantec Protection Center may change over time. For the latest information about supported products, see the Symantec Support Web site.

See "Configuring Symantec Protection Center to manage products" on page 49.

See "Logging on to Symantec Protection Center" on page 45.

See "Symantec Protection Center architecture" on page 44.

Symantec Protection Center architecture

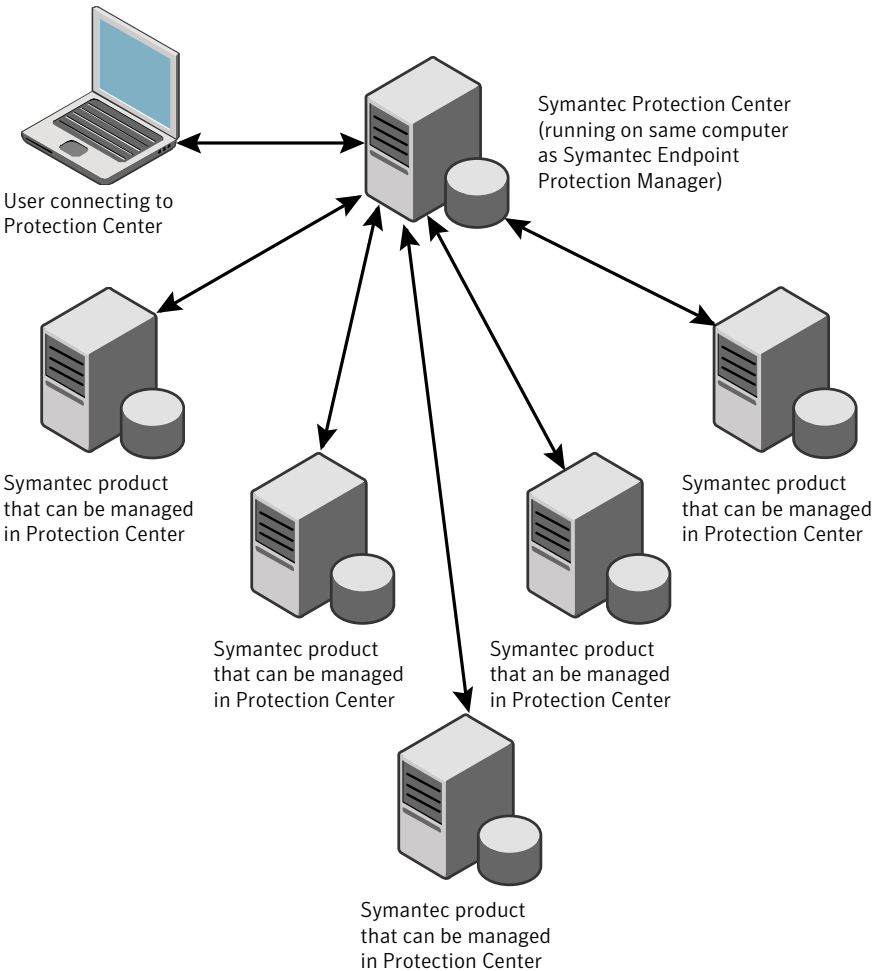
Symantec Protection Center provides integrated access to individual Symantec product management consoles and reports. Individual product servers and databases, however, remain separate. Protection Center does not offer data integration across products.

See "About Symantec Protection Center" on page 43.

Protection Center communicates with integrated products according to the communication settings that individual products require. You specify these settings when you configure Protection Center to manage your products.

See "Configuring Symantec Protection Center to manage products" on page 49.

Figure 3-1 Symantec Protection Center architecture



Logging on to Symantec Protection Center

Symantec Protection Center is installed with a default Administrator account. The first time that you start Protection Center, you log on with a default user name and password. You then must change the password.

To log on to Protection Center

1. In Internet Explorer, go to https://<*hostname*>:9090, where <*hostname*> is the IP address or computer name of the server where Symantec Endpoint Protection Manager is installed.

   If Symantec Endpoint Protection Manager is installed on this computer, you can also click **Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Web Access**.

2. Click the link to launch Symantec Protection Center.

   If the Web page security certificate warning appears, click **Continue to this website (not recommended)** and add the self-signed certificate to Internet Explorer.

   This message means that Internet Explorer does not recognize the linked site as being secure. Internet Explorer relies on security certificates to determine if a site is secure.

   For instructions to add the security certificate to Internet Explorer, see the Symantec Technical Support Knowledge Base article, How to add the self-signed certificate for Symantec Protection Center or Symantec Endpoint Protection Manager to Internet Explorer.

3. On the Protection Center Dashboard, enter the user name and password.
   - Default user name: **admin**
   - Default password: **admin**

4. When you log on for the first time with the default user name and password, on the **Change Password** page, type the required information.

   Document your changed password and store it in a secure location. You can recover the password only if you set up another Administrator account.

See "About managing Symantec Protection Center accounts" on page 47.

The Symantec Protection Center Dashboard

The Symantec Protection Center home page is called the Dashboard. When you log on to Protection Center for the first time, the Dashboard provides only global security threat information. After you integrate your products with Protection Centers, the Dashboard reports on the overall health of your network security, based on the products that you integrate.

From the Dashboard, you can navigate directly to the following pages:

- Individual product management consoles

- Reports for your products
  See "Symantec Protection Center Reports" on page 50.
- Settings management for Symantec Protection Center accounts and integrated products
  See "About managing Symantec Protection Center accounts" on page 47.
  See "Configuring Symantec Protection Center to manage products" on page 49.

About managing Symantec Protection Center accounts

Symantec Protection Center is installed with a default Administrator account. After you log on for the first time, you can create additional accounts and register sets of products to each account. You can delete the default Administrator account only after you create another Administrator account.

See "Logging on to Symantec Protection Center" on page 45.

With a Protection Center Administrator account, you can create additional Protection Center accounts with limited settings. The following table explains the Protection Center account types:

Administrator Account	■ Can access all product functionality that is associated with the product accounts for this Protection Center account ■ Can create and delete Protection Center accounts ■ Can change Protection Center account settings for all accounts. This includes changing passwords ■ Can add integrated products to Protection Center for all accounts **Note:** To mitigate the risk of lost passwords, you can create more than one Administrator account. A Protection Center Administrator can change the password for another account without knowing the original password.
Standard Account	■ Can access all product functionality that is associated with the product accounts for this Protection Center account ■ Can change Protection Center account settings for this account only ■ Can add integrated products to Protection Center for this account only

Product registration is specific to each Protection Center user account. You must register a set of products for each Protection Center user.

The access that a Protection Center account provides to individual product functionality depends on the product account that is used to register the product with Protection Center.

For example, you can register Symantec Endpoint Protection Manager with a Protection Center Standard account by using a Symantec Endpoint Protection Manager system administrator account. The user of this account can then perform the following tasks:

- Modify only their own account settings in Protection Center
  They cannot create other Protection Center accounts of any type.
- Create and modify any type of Symantec Endpoint Protection Manager account in the Symantec Endpoint Protection Manager console that they access through Protection Center
  Perform all tasks in Symantec Endpoint Protection Manager.

Similarly, you can register Symantec Endpoint Protection Manager with a Protection Center Administrator account by using a Symantec Endpoint Protection Manager limited administrator account. The user of this account can then perform the following tasks:

- Create and modify any account in Protection Center
- Perform only limited tasks in Symantec Endpoint Protection Manager
  They cannot create or modify any Symantec Endpoint Protection Manager accounts.

Note: At a minimum, if you register Symantec Endpoint Protection Manager with a limited administrator account, the account must include reporting rights.

See "Configuring Symantec Protection Center to manage products" on page 49.

You can change your Protection Center account settings at any time. After you register a product in Symantec Protection Center, you can easily change the product settings or remove the product completely.

See "About Symantec Protection Center" on page 43.

Configuring Symantec Protection Center to manage products

You configure Symantec Protection Center to manage your integrated products by registering or adding each product to Protection Center. You can perform this task at any time after you install and configure the individual products.

During the registration process, you provide the logon credentials for each product. The credentials allow Protection Center to connect and communicate with your other Symantec products. After you register or add your products to Protection Center, you are automatically logged on to all your products when you log on to Protection Center.

See "About Symantec Protection Center" on page 43.

If you customized any communication settings when you installed your products, you must specify the settings when you register the products. These settings include the following:

- Whether to require a secure connection for product information
- Custom ports
  The default port numbers are 8014 for the product logon, the product dashboard, and the product reports, and 8443 for the product console.

Note: If you use a limited administrator account to register Symantec Endpoint Protection Manager with Protection Center, the account must include reporting rights.

See "About administrators" on page 293.

See "Configuring the access rights for a limited administrator" on page 298.

Note: Product registration is specific to each Protection Center user account. You must register a set of products for each Protection Center user account.

See "About managing Symantec Protection Center accounts" on page 47.

To configure Protection Center to manage products

1. On the Symantec Protection Center Dashboard, or on the main **Settings** page, click **Add a product to manage**.
2. Enter the requested information in the appropriate fields. You must provide the following information:

New product display name	Any string that you want to use to identify your product in Protection Center
Product type	Select your product from the drop-down list.
Product address	The IP address of the server where you installed the version of your product that you want to register. You can also enter a computer name.
Product user name	The user name for the administrator account for your product
Product password	The password for the administrator account for your product

3. If you customized any communication settings when you installed the product, click **Product communication settings** and specify the appropriate settings.
4. Click **Test Connection** to make sure that Protection Center can communicate with your product.
5. Click **Add Product**.

Symantec Protection Center Reports

The Symantec Protection Center Reports page lets you run reports for your integrated products directly from the Protection Center console. You do not need to navigate to the individual product consoles to run reports.

These reports are all the same ones that are available in your standalone products. For more information, see your individual product documentation.

If you run a report and no data appears, try refreshing your browser.

See "About Symantec Protection Center" on page 43.

About Symantec Protection Center documentation

Symantec Protection Center includes Help, which you can access from the Help link in the Protection Center window.

The Protection Center documentation explains only how to use the features of Protection Center itself. For information about the products that can integrate with Protection Center, refer to the individual product documentation.

When you access your individual product consoles in Protection Center, you can also access the product Help from within the console.

For example, if you run the Symantec Endpoint Protection Manager console in Symantec Protection Center, you have access to all the features and functions of the product console. This access includes the Symantec Endpoint Protection documentation and Help.

See "About Symantec Protection Center" on page 43.

Chapter 4

Managing groups and clients

This chapter includes the following topics:

- Viewing the status of clients and client computers
- Filtering which clients you can view on the Clients tab
- Restarting client computers
- Viewing a client's properties
- Searching for information about clients
- Configuring a client to detect unknown devices
- Running commands on clients from the console

Managing computer groups

In Symantec Endpoint Protection Manager, you can manage groups of client computers as a single unit.

Table 4-1 describes the actions that you can perform when you manage your groups of computers.

Table 4-1 Group management actions

Task	Description
Create a group	You can read about groups and how to create them. The newly created groups are listed as child groups under the **My Company** parent group. See "How you can structure groups" on page 55. See "Adding a group" on page 57.
Import existing groups	If your organization already has an existing group structure, you can import the groups as organizational units. See "Importing an existing organizational structure" on page 57.
Disable inheritance for subgroups	The subgroups inherit the same security settings from the parent group by default. You can disable inheritance. You can disable inheritance between a subgroup and a parent group. See "Disabling and enabling a group's inheritance" on page 60.

Table 4-1 Group management actions *(continued)*

Task	Description
Manage security policies for groups	You can create security policies based on the needs of each group. You can then assign different policies to different groups. See "Using policies to manage your network security" on page 90.
Create locations within groups	You can set up the clients to switch automatically to a different security policy if the physical location of the client changes. See "Using location awareness with groups" on page 79. Some security settings are group-specific and some settings are location-specific. You can customize any settings that are location-specific. See "Configuring communication settings for a location" on page 182.
View a group's properties	You can view the groups to check whether the client computers are in the correct group. You can also check the policy number that is assigned to the group. See "Viewing a group's properties" on page 60.
Move a group	You can move one subgroup to another group if you want to automatically inherit the policies of the new group. See "Moving a group" on page 59.
Add and manage the client computers	You can manage clients from the group. For example, you can add clients to a group, run and monitor endpoint protection, and view information about the clients. See "Setting up and managing clients in groups" on page 61.

How you can structure groups

In Symantec Endpoint Protection Manager, groups function as a container for client computers. You organize computers with similar security needs into groups to make it easier to manage network security.

Symantec Endpoint Protection Manager 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 **Default Group** is a subgroup to **My Company**. Clients are first assigned to the **Default Group** when they first register with Symantec Endpoint Protection Manager, unless they belong to a predefined group. You cannot create subgroups under the **Default Group**

You cannot rename or delete the default groups.

You can create multiple subgroups to match the organizational structure of your company. You can base your group structure on function, role, geography, or a combination of criteria.

Table 4-2 Criteria for creating groups

Criterion	Description
Function	You can create groups based on the types of computers to be managed, such as laptops, desktops, and servers. Alternatively, you can create multiple groups that are based on usage type. For example, you can create a Mobile group for the computers whose users travel and Local for the computers in the office.
Role	You can create groups for department roles, such sales, engineering, finance, and marketing.
Geography	You can create groups based on the offices, cities, states, regions, or countries where the computers are located.
Combination	You can create groups based on a combination of criteria. For example, you can use the function and the role. You can add a parent group by role and add child subgroups by function, as in the following scenario: ■ Sales, with subgroups of laptops, desktops, and servers. ■ Engineering, with subgroups of laptops, desktops, and servers.

For example, suppose that a company has telemarketing and accounting departments. These departments have staff in the company's New York, London, and Frankfurt offices. All computers in both departments are assigned to the same group so that they receive virus and security risk definitions updates from the same source. However, IT reports indicate that the telemarketing department is more vulnerable to risks than the accounting department. As a result, the system administrator creates separate telemarketing and accounting groups. Telemarketing clients share configuration settings that strictly limit how users can interact with their antivirus and security risk protection.

See "Managing computer groups" on page 54.

Adding a group

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

Group descriptions may be up to 1024 characters long. Group names may contain any character except the following characters: [" / \ * ? < > | :] Group descriptions are not restricted.

Note: You cannot add groups to the Default Group.

See "How you can structure groups" on page 55.

To add a group

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

Importing an existing organizational structure

You can import and synchronize information about user accounts and computer accounts from an Active Directory server or an LDAP directory server. You can import group structures, or Organizational Units (OUs). Symantec Endpoint Protection can then automatically synchronize the groups on the Clients tab with those on the directory server.

You cannot use the Clients tab to manage these groups after you import them. You cannot add, delete, or move groups within an imported OU.

You can assign security policies to the imported OU. You can also copy users from an imported organizational unit to other groups that are listed in the View Clients pane. The policy that was assigned to a group before the group was imported has priority. A user account can exist in both the OU and in an outside group. The policy that was applied to the outside group has priority.

Table 4-3 Tasks for importing Organizational Units

Task	Description
Plan for importing Organizational Units	You can plan how you want the Symantec Endpoint Protection Manager to automatically synchronize users, computers, and the entire group structure in an OU from an Active Directory or LDAP server. See "About organizational units and the LDAP server" on page 325.
Add a directory server	You cannot filter the users from an Active Directory server before you import data. With LDAP servers, you can filter the users before you import data. Therefore you may want to add an Active Directory server that has LDAP compatibility as an LDAP server if you need to filter the data. See "Adding directory servers" on page 319.
Synchronize information about user accounts and computer accounts between directory servers and a Symantec Endpoint Protection Manager	You can import and synchronize information about user accounts and computer accounts between directory servers and Symantec Endpoint Protection Manager. See "Synchronizing user accounts between directory servers and a Symantec Endpoint Protection Manager" on page 321.
Search for users on an LDAP directory server	When you import information about users to the management server, you need to search for users on an LDAP server. See "Searching for users on an LDAP directory server" on page 322.
Import users from an LDAP directory server search results list	You can import users from an LDAP server search results list. See "Importing users from an LDAP directory server search results list" on page 324.
Import organizational units from an Active Directory server or an LDAP directory server	You can import OUs from an Active Directory server or an LDAP directory server. See "Importing organizational units from an active or LDAP directory server" on page 325.

Table 4-3 Tasks for importing Organizational Units *(continued)*

Task	Description
Import user account and computer account information from an LDAP server	You can import user account and computer account information from an LDAP server. See "About importing user and computer account information from an LDAP directory server" on page 321.
Synchronize Organizational Units	You can synchronize OUs. See "About synchronizing organizational units" on page 325.

Renaming a group

You can rename groups and subgroups to reflect changes in your organizational structure. You can rename a group to automatically update that group's name for all the users and the computers that are already assigned to that group. The client computers in a renamed group are not forced to switch groups or to download a new group profile.

See "Managing computer groups" on page 54.

To rename a group

1. In the console, click **Clients**.
2. On the **Clients** tab, under **View Clients**, right-click the group that you want to rename, and then click **Rename**.
3. In the **Rename Group for *group name*** dialog box, type the new group name.
4. Click **OK**.

Moving a group

Any group along with its subgroups, computers, and users, can be moved from one node of the group tree to another. However, neither the My Company group nor the Default Group can be moved. In addition, you cannot move groups under the Default Group, or move a group under one of its subgroups.

If a group uses an inherited policy, it takes on the new inherited policy of the group to which it moves. If it has a specific policy applied, it keeps that policy after the move.

If there is no group policy explicitly applied to the group you move, it uses the group policy of the destination group. The clients in the group you move use the new profile.

See "Managing computer groups" on page 54.

To move a group

1. In the console, click **Clients**.
2. On the **Clients** tab, under **View Clients**, right-click the group you want to move and click **Move**.
3. In the **Move Group** dialog box, select the destination group to which you want to move the group.
4. Click **OK**.

Viewing a group's properties

Each group has a property page that lists some information about the group that you might need to check. It contains the date that the group was last modified and its policy serial number. It also lists the number of computers in the group and the number of registered users. From this dialog box, you can block new clients from being added to the group.

See "Managing computer groups" on page 54.

To view a group's properties

1. In the console, click **Clients**.
2. In the **View Clients** pane, choose the group whose properties you want to view.
3. Click the **Details** tab.

Disabling and enabling a group's inheritance

In the group structure, subgroups initially and automatically inherit the locations, policies, and settings from their parent group. By default, inheritance is enabled for every group. You can disable inheritance so that you can configure separate security settings for a subgroup. If you make changes and later enable inheritance, any changes that you made in the subgroup's settings are overwritten.

See "Managing computer groups" on page 54.

To disable or enable a group's inheritance

1. In the console, click **Clients**.
2. On the **Clients** page, under **View Clients**, select the group for which you want to disable or enable inheritance.

   You can select any group except the top-level group, My Company.
3. In the ***group name*** pane, on the **Policies** tab, do one of the following tasks:
   - To disable inheritance, uncheck **Inherit policies and settings from parent group "*group name*"**.
   - To enable inheritance, check **Inherit policies and settings from parent group "*group name*"**, and then click **Yes** when asked to proceed.

Setting up and managing clients in groups

A client is any network device that connects to the network and runs the Symantec Endpoint Protection software. Network devices can include laptops, desktop computers, and servers. A Symantec Endpoint Protection client software package is deployed to each device in the network to protect it.

The client software performs the following functions on the clients:

- Connects to the management server to receive the latest policies and configuration settings.
- Applies the settings in each policy to the computer.
  See "About the types of protection" on page 33.
- Updates the latest content and virus and security risk definitions on the computer.
- Records client information in its logs and uploads the logs' information to the management server.

You can configure clients in Symantec Endpoint Protection Manager in a number of different ways.

Table 4-4 Tasks related to clients that you may want to perform

Task	Description
Add clients to groups	You can add clients to groups as users or as computers. See "Preassigning computers or users to groups before you install the client software" on page 64. See "About user mode and computer mode" on page 63.

Table 4-4 Tasks related to clients that you may want to perform *(continued)*

Task	Description
View the status of clients	You can monitor the real-time operational status of the clients in your network. See "Viewing the status of clients and client computers" on page 69.
View a client's properties	You can view the hardware and the network properties of each client, such as group, domain, logon name, and software version. If you have enabled user information collection, you can also see information about the user who is currently logged on to the computer. See "Viewing a client's properties" on page 72.
Filter the clients that appear on the **Clients** tab	You can use a filter to control which clients appear on the **Clients** tab. This feature is particularly useful if you have a large number of clients. See "Filtering which clients you can view on the Clients tab" on page 71.
Search for information about clients	You can search for information about clients, such as the operating system version and the antivirus definitions version in use on the computer. See "Searching for information about clients" on page 73.
Switch clients between user mode and computer mode	You can switch clients from users to computers or from computers to users. See "Switching a client between user mode and computer mode" on page 66.
Convert a self-managed client to a managed client	If a user installs the client software from an installation CD, the client is unmanaged and does not communicate with the management server. You can change self-managed clients into managed ones. See "Converting an unmanaged client to a managed client" on page 66.
Change the client's user control level	A client's user control level determines which Network Threat Protection features and client user interface settings are available for users to configure. See "Changing the user control level" on page 165.

Table 4-4 Tasks related to clients that you may want to perform *(continued)*

Task	Description
Run commands on clients from the console	You can run commands on a client or a group from the console. See "Running commands on clients from the console" on page 76.
Move clients from group to group	You can change the group that a client is in. See "Moving clients between groups" on page 69.
Block clients from being added to groups	You can prevent a client from automatically being added to a group. You can block clients if you do not want them to be added automatically to a specific group when they connect to the network. See "Blocking clients from being added to groups" on page 68.
Set up clients to detect unauthorized devices	Clients that you add in computer mode can be enabled as unmanaged detectors and used to detect unauthorized devices. See "Configuring a client to detect unknown devices" on page 74.

About user mode and computer mode

You configure clients to be in either user mode or computer mode, based on how you want to apply policies to the clients in groups. When you add a client, it defaults to computer mode, which takes precedence over user mode.

If the client software runs in user mode, the client computer gets the policies from the group of which the user is a member. If the client software runs in computer mode, the client computer gets the policies from the group of which the computer is a member. Many organizations configure a majority of clients in computer mode. Based on your network environment, you might want to configure a few clients with special requirements as users.

You set up clients as users or computers by adding the users and computers to an existing group. After a user or a computer is added to a group, it assumes the policies that were assigned to the group.

Mode	Description
Computer mode	The client protects the computer with the same policies, regardless of which user is logged on to the computer. The policy follows the group that the computer is in. Computer mode is the default setting.
User mode	The policies change, depending on which user is logged on to the client. The policy follows the user.

See "Preassigning computers or users to groups before you install the client software" on page 64.

Clients that you add in computer mode can be enabled as unmanaged detectors, and used to detect unauthorized devices.

See "Configuring a client to detect unknown devices" on page 74.

Preassigning computers or users to groups before you install the client software

After you install the client software on a computer, the client receives the policies from the group that is specified in the client installation package. You might not want the client to receive the package's group policies. Instead, you can first add a placeholder for the client in a selected group, and install the client software later. The client remains in the group you added a placeholder for, and not the group that is specified in the client installation package.

See "About groups specified in the client installation package" on page 65.

You add the client based on a user name or a computer name. You cannot add the client to more than one group.

See "About user mode and computer mode" on page 63.

See "Setting up and managing clients in groups" on page 61.

Note: Make sure that the management server does not block new clients from being added to a group.

See "Blocking clients from being added to groups" on page 68.

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

See "Deploying client software with Find Unmanaged Computers" on page 125.

To preassign computers or users to groups before you install the client software

1. In the console, click **Clients**.
2. On the **Clients** page, under **View Clients**, locate the group to which you want to add a client.
3. On the **Clients** tab, under **Tasks**, do one of the following actions:
   - For user mode, click **Add User Account**. Enter the user name. If the user is part of a Windows Domain, type the domain name. If the user is part of a workgroup, click **Log on local computer**.
   - For computer mode, click **Add Computer Account**. Type the computer name and then type the Windows Domain name or type `Workgroup`.

   For more information on these options, click **Help**.
4. Click **OK**.

About groups specified in the client installation package

When you create a client installation package for deployment, you can specify which group you want the client computer to be a member of. After you install the client installation package on the computer, the client computer becomes a member of this preferred group. However, the management server can override the preferred group setting. For example, you can add a client in computer mode for the client on the Clients page. You might add the computer under a different group than the preferred group in the client installation package. After the client connects to the management server, the group you added the client to overrides the preferred group.

See "Preassigning computers or users to groups before you install the client software" on page 64.

The server may not allow the client to join the preferred group for any of the following reasons:

- The preferred group does not exist or has been deleted.
  The client is placed in the Default Group.
- The client is a new client, but the server blocks the client from being added to a group.
  The client is placed in the Default Group.
  See "Blocking clients from being added to groups" on page 68.
- The client was previously registered to another group and you try to move the client to a new group by using the **Export Communication Settings** command.

The client stays in the original group.
See "Converting an unmanaged client to a managed client" on page 66.

Switching a client between user mode and computer mode

You can configure clients to run in either user mode or computer mode. In user mode, the client computer that a user logs on to uses the policy of the group to which the user belongs. In computer mode, the client computer uses the policy of the group to which the computer belongs. In computer mode, the applied policy is independent of the user who logs on to the computer.

See "About user mode and computer mode" on page 63.

You cannot switch from user mode to computer mode if the computer name is already in any group. Switching to computer mode deletes the user name of the client from the group and adds the computer name of the client into the group.

You cannot switch from computer mode to user mode if the user's logon name and the computer name are already contained in any group. Switching to user mode deletes the computer name of the client from the group. It then adds the user name of the client into the group.

To switch a client between user mode and computer mode

1. In the console, click **Clients**.
2. On the Clients page, under **View Clients**, select the group that contains the user or computer.
3. On the Clients tab, right-click the computer or the user name in the table, and then select either **Switch to Computer Mode** or **Switch to User Mode**.

   This mode is a toggle setting so one or the other always displays. The information in the table changes to reflect the new setting.

Converting an unmanaged client to a managed client

If a user installed a client from the installation CD, the client is unmanaged and does not communicate with the management server.

You can convert the unmanaged client to a managed client by using the following process:

- You export a file that includes all the communication settings for the group that you want the client to be in.
  The default file name is *group name*_sylink.xml.

- You deploy the file to the client computer.
  You can either save the file to a network location or send it to an individual user on the client computer.
- On the client computer, you or the user imports the file.
  You do not need to restart the client computer.

The client immediately connects to the management server. The management server places the client in the group that is specified in the communication file. The client is updated with the group's policies and settings. After the client and the management server communicate, the notification area icon with the green dot appears in the client computer's taskbar.

Unmanaged clients are not password-protected, so the user does not need a password on the client. However, if the user tries to import a file onto a managed client that is password-protected, then the user must enter a password. The password is the same one that is used to import or export a policy.

See "Password-protecting the client" on page 170.

You may also need to redirect a managed client to another server.

See "Recovering client communication settings by using the SylinkDrop tool" on page 188.

See "Assigning a management server list to a group and location" on page 177.

To export the communications settings from the server

1. In the console, click **Clients**.
2. Under **View Clients**, select the group in which you want the client to appear.
3. Right-click the group, and then click **Export Communication Settings**.
4. In the Export Communication Settings for *group name* dialog box, click **Browse**.
5. In the **Select Export File** dialog box, locate the folder to where you want to export the .xml file, and then click **OK**.
6. In the Export Communication Settings for *group name* dialog box, select one of the following options:
   - To apply the policies from the group from which the computer is a member, click **Computer Mode**.

- To apply the policies from the group from which the user is a member, click **User Mode**.

7 Click **Export**.

If the file name already exists, click **OK** to overwrite it or **Cancel** to save the file with a new file name.

To finish the conversion, you or a user must import the communications setting on the client computer.

To import the server communications settings into the client

1 Open Symantec Endpoint Protection on the computer that you want to convert to a managed client.

2 In the upper right, click **Help and Support**, and then click **Troubleshooting**.

3 In the **Troubleshooting** dialog box, under **Communication Settings**, click **Import**.

4 In the **Import Communication Settings** dialog box, locate the *group name_sylink*.xml file, and then click **Open**.

5 Click **Close** to close the **Troubleshooting** dialog box.

After you import the communications file, and the client and the management server communicate, the notification area icon with appears in the computer's taskbar. The green dot indicates that the client and the management server are in communication with each other.

Blocking clients from being added to groups

You can set up client installation packages with their group membership already defined. If you define a group in the package, the client automatically is added to the appropriate group. The client is added the first time it makes a connection to the management server.

See "Using client installation packages" on page 119.

You can turn on blocking if you do not want clients to be added automatically to a specific group when they connect to the network.

Note: The blocking option prevents users from automatically being added to a group. You can block a new client from being added to the group to which they were assigned in the client installation package. In this case the client gets added to the Default Group. You can manually move a user or a computer to a blocked group.

To block clients from being added to groups

1. In the console, click **Clients**.
2. Under **View Clients**, select the group for which you want to block new clients.
3. Click the **Details** tab.
4. On the **Details** tab, under **Tasks**, click **Edit Group Properties**.
5. In the **Group Properties for *group name*** dialog box, click **Block New Clients**.
6. Click **OK**.

Moving clients between groups

You can move clients between groups and subgroups. The client switches to the new group after you move the client.

You cannot move clients within an organizational unit. You can copy clients from an organizational unit to Symantec Endpoint Protection Manager groups.

See "Managing computer groups" on page 54.

To move clients between groups

1. In the console, click **Clients**.
2. On the **Clients** page, under **View Clients**, locate the group that contains the clients that you want to move.
3. On the **Clients** tab, right-click the clients you want to move and click **Move**.

   Use the Shift key or the Control key to select all clients or specific clients.
4. In the **Move Group: *group name*** dialog box, select the group to which you want to move the selected clients.
5. Click **OK**.

Viewing the status of clients and client computers

You can view information about the real-time operational status of the clients and the computers in your network. For example, you can view which clients have the latest policies and definitions. You can see a computer's IP address or which computers run a particular operating system.

Table 4-5 Client and computer status views

View	Description
Default view	Displays a list of managed clients, user accounts, and the computer accounts that do not have the client installed. You can view the computer name, the domain name, and the name of the user who is logged on. Default is the default view. The Name column displays icons next to each client to indicate whether the clients are connected to the management server. See "Viewing the client health state in the management console" on page 180.
Client status	Displays the information about the client, such as the group's policy serial number and the client's version number.
Protection technology	Indicates whether Antivirus and Antispyware Protection, Network Threat Protection, and Auto-Protect are turned on or turned off. This view also displays the date and the revision number of the latest signatures and content.
Network information	Displays the information about the client computer's network components, such as the MAC address of the network card that the computer uses.
Client system	Displays the system information about the client computer, such as the amount of available disk space and the operating system version number.

After you know the status of a particular client, you can resolve any security issues on the client computers. For example, you might have to download the latest antivirus definitions. Or you can run commands remotely from each group, such as to enable Auto-Protect.

See "Running commands on clients from the console" on page 76.

You can also run scheduled quick reports with the status information.

See "Creating quick reports" on page 250.

You can also view most of this information by right-clicking each client, and then by clicking **Properties**. The only field that you can edit is the Description field on the General tab.

See "Viewing a client's properties" on page 72.

See "Filtering which clients you can view on the Clients tab" on page 71.

To display the status of clients and client computers

1. In the console, click **Clients**.
2. On the Clients page, under **View Clients**, locate the group that contains the clients that you want information about.
3. On the Clients tab, click the **View** drop-down list, and then select a category.

   You can go directly to a particular page by typing the page number in the text box at the bottom right-hand corner.

Filtering which clients you can view on the Clients tab

You can display which clients in a group appear on the **Clients** tab, based on the operating system or account type. You can display or hide which computers are connected to the management server. You can also configure how many clients appear on each page to make the list easier to manage.

See "Viewing the status of clients and client computers" on page 69.

See "Viewing the client health state in the management console" on page 180.

To display which users and computers you can view on the Clients tab

1. In the console, click **Clients**.
2. In the **View Clients** pane, choose the group you want to search on.
3. On the **Clients** tab, under **Tasks**, click **Change Clients View**.
4. In the **Change Clients View** dialog box, under **Platform type**, select whether you want to display Windows computers, Mac computers, or both

   See "About user mode and computer mode" on page 63.
5. Under **Account type**, select whether you want to display clients in user mode or computer mode.
6. Check the following options, if desired:
   - **New computers or users that do not have the client software installed**
   - **Online status**
7. To shorten the list, click **Results per page** and enter the number of results to show on each page.

   Valid values range from 1 to 1000.
8. Click **OK**.

Restarting client computers

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

See "Running commands on clients from the console" on page 76.

To restart a selected client computer

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

Viewing a client's properties

Each user and computer has a property page. The only field that you can edit is the Description field on the General tab.

The page includes the following tabs:

- General
  Displays the information about the group, domain, logon name, and the hardware configuration of the computer.
- Network
  Displays the information about the DNS server, DHCP server, WINS server, and the IP address of the computer.
- Clients
  Displays the information that is gathered from the client computer. This information includes the type of client that runs on the computer. In addition, it lists specific software and policy information. This information includes client software version, the current profile serial number, the current signature serial number, and the last online time.
- User Info
  Displays the information about the person currently logged on the computer. This information is populated when the administrator chooses to enable the collection of user information.

See "Collecting user information" on page 122.

To view a client's properties

1. In the console, click **Clients**.
2. In the View Clients pane, choose the group with the clients whose properties you want to view.
3. On the Clients tab, select the client.
4. Under Tasks, click **Edit Properties**.
5. In the *client name* dialog box, you can view information about the client.
6. Click **OK**.

Searching for information about clients

You can search for information about the clients, client computers, and users to make informed decisions about the security of your network. For example, you can find which computers in the Sales group run the latest operating system. Or, you can find out which client computers in the Finance group need the latest antivirus definitions installed. You can view the information about each client in the group on the Clients page. You can narrow down the search if there are too many clients.

See "Viewing the status of clients and client computers" on page 69.

You can export the data that is contained in the query into a text file.

Note: To search for most of the information about the users, you must collect user information during the client software installation or later. This user information is also displayed on the General tab and the User Info tab in the client's Edit Properties dialog box.

See "Collecting user information" on page 122.

See "Viewing a group's properties" on page 60.

To search for information about users, clients, and computers

1. In the console, click **Clients**.
2. On the Clients tab, under View Clients, choose the group you want to search.
3. Under Tasks, click **Search Clients**.
4. In the Search for Clients dialog box, in the Find drop-down list, click either **Computers** or **Users**.

5 Click **Browse** to select a group other than the default group.

6 In the Select Group dialog box, select the group, and then click **OK**.

7 Under Search Criteria, click the Search Field drop-down list, and then select the criteria by which you want to search.

8 Click the Comparison Operator drop-down list, and then select a comparison operator.

You can use standard Boolean operators in your search criteria.

9 In the Value cell, type the search string.

10 Click **Search**.

You can export the results into a text file.

11 Click **Close**.

Configuring a client to detect unknown devices

Unauthorized devices can connect to the network in many ways, such as physical access in a conference room or rogue wireless access points. To enforce policies on every endpoint, you must be able to quickly detect the presence of new devices. Unknown devices are the devices that are unmanaged and that do not run the client software. You must determine whether the devices are secure. You can enable any client as an unmanaged detector to detect the unknown devices.

When a device starts up, its operating system sends ARP traffic to the network to let other computers know of the device's presence. A client that is enabled as an unmanaged detector collects and sends the ARP packet information to the management server. The management server searches the ARP packet for the device's MAC address and the IP address. The server compares these addresses to the list of existing MAC and IP addresses in the server's database. If the server cannot find an address match, the server records the device as new. You can then decide whether the device is secure. Because the client only transmits information, it does not use additional resources.

You can configure the unmanaged detector to ignore certain devices, such as a printer. You can also set up email notifications to notify you when the unmanaged detector detects an unknown device.

To configure the client as an unmanaged detector, you must do the following actions:

- Enable Network Threat Protection.
  See "Enabling and disabling Network Threat Protection" on page 498.
- Switch the client to computer mode.

See "Switching a client between user mode and computer mode" on page 66.

- Install the client on a computer that runs all the time.
- Enable only Symantec Endpoint Protection clients as unmanaged detectors. A Symantec Network Access Control client cannot be an unmanaged detector.

To configure a client to detect unauthorized devices

1. In the console, click **Clients**.
2. Under **View Clients**, select the group that contains the client that you want to enable as an unmanaged detector.
3. On the **Clients** tab, right-click the client that you want to enable as an unmanaged detector, and then click **Enable as Unmanaged Detector**.
4. To specify one or more devices to exclude from detection by the unmanaged detector, click **Configure Unmanaged Detector**.
5. In the **Unmanaged Detector Exceptions for *client name*** dialog box, click **Add**.
6. In the **Add Unmanaged Detector Exception** dialog box, click one of the following options:
   - **Exclude detection of an IP address range**, and then enter the IP address range for several devices.
   - **Exclude detection of a MAC address**, and then enter the device's MAC address.
7. Click **OK**.
8. Click **OK**.

To display the list of unauthorized devices that the client detects

1. In the console, click **Home**.
2. On the **Home** page, in the **Security Status** section, click **More Details**.
3. In the **Security Status Details** dialog box, scroll to the **Unknown Device Failures** table.
4. Close the dialog box.

   You can also display a list of unauthorized devices on the **Unknown Computers** tab of the **Find Unmanaged Computers** dialog box.

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

Running commands on clients from the console

You can run commands remotely on individual clients or an entire group from the Symantec Endpoint Protection Manager console. On managed clients, the commands that you run override the commands that the user runs.

You can run the commands from the Clients tab or the Monitors tab in the console.

See "Running commands and actions from logs" on page 274.

You can configure a limited administrator to have rights to some or none of these commands. By default, a limited administrator has rights to all commands except **Restart Client Computers**.

See "Configuring the access rights for a limited administrator" on page 298.

Note: All the listed commands are displayed in the console user interface. Some of them, however, are not recognized by Mac client computers.

Table 4-6 Commands that you can run on clients

Commands	Description
Scan	Runs on-demand scan on the clients. See "Running on-demand scans" on page 453.
Cancel All Scans	Cancels all the scans that currently run on the clients.
Update Content	Updates content on clients by initiating a LiveUpdate session on the clients. The clients receive the latest content from Symantec LiveUpdate. See "Running LiveUpdate on a client from the console" on page 162.
Update Content and Scan	Updates content by initiating a LiveUpdate session and runs an on-demand scan on clients. See "Running LiveUpdate on a client from the console" on page 162.
Restart Client Computers	Restarts the clients. See "Restarting client computers" on page 72.
Enable Auto-Protect	Enables File System Auto-Protect on the clients. See "Enabling File System Auto-Protect" on page 430.

Table 4-6 Commands that you can run on clients *(continued)*

Commands	Description
Enable Network Threat Protection	Enables Network Threat Protection on the clients. See "Enabling and disabling Network Threat Protection" on page 498. **Note:** This command is not recognized by a Mac client computer.
Disable Network Threat Protection	Disables Network Threat Protection on the clients. See "Enabling and disabling Network Threat Protection" on page 498. **Note:** This command is not recognized by a Mac client computer.

Chapter 5

Managing a group's locations

This chapter includes the following topics:

Using location awareness with groups

Employees frequently need to connect to the network from multiple locations, such as their homes, Internet cafés, hotels, and the office. Different locations may have different security needs.

You can create locations and assign a separate security policy to different locations based on the following criteria:

- The type of network connection, such as wireless, Ethernet, or VPN.
- The location of the connection.

You may want to add several locations that reflect the following kinds of connections:

- Wireless connections inside the office.

- Non-wireless connections inside the office.
- Connections from remote corporate locations outside of the office.
- VPN connections from outside of the office.

You add locations after you have set up all the groups that you need to manage. Each group can have different locations if your security strategy requires it. In the Symantec Endpoint Protection Manager console, you can set up the conditions that trigger automatic policy switching based on location. When you enable location awareness, it automatically applies the best security policy to a client or server, based on the location from which a user connects.

You can add a set of conditions to each group's locations that automatically selects the correct security policies for a user's environment. These conditions are based on criteria such as the network settings of the computer from which the request for network access was initiated. An IP address, a MAC address, or the address of a directory server can also function as condition. If you change a security policy in the console, either the management server updates the policy on the client or the client downloads the policy.

If the current location is not valid after the update, then the client either:

- Switches to another location that is valid.
- Uses the default location.

You can customize the policy and settings of each location. For example, the policies for an office location may not need to be as strict as the policies for a VPN or home location. The policy that is associated with the default location is used when the user is already behind a corporate firewall.

When you create a location, it applies to the group for which you created it and any groups that inherit from the parent group. You should create the locations that you intend to apply to all clients at the My Company group level. You can create some locations that are specific to a particular group. For example, in most companies all clients require a default location that is added automatically to the My Company group. However, not all clients require a VPN connection. You can set up a separate group that is called Telecommuters for the clients who require a VPN connection. You add the VPN location to the Telecommuters group as well as to the inherited office location. Clients in that group can then use the policies that are associated with either the office or the VPN location.

Table 5-1 Location awareness tasks that you can perform

Tasks	Description
Plan locations	You should consider the different types of security policies that you need in your environment to determine the locations that you should use. You can then determine the criteria to use to define each location. See "About planning locations" on page 82.
Enable location awareness	To control the policies that are assigned to clients contingent on the location from which the clients connect, you can enable location awareness. See "Enabling location awareness for a client" on page 83.
Add locations	You can add locations to groups. See "Adding a location with a wizard" on page 84. See "Adding a location without a wizard" on page 86.
Assign default locations	All groups must have a default location. When you install the console, there is only one location, called Default. When you create a new group, its default location is always Default. You can change the default location later after you add other locations. The default location is used if one of the following cases occurs: ■ One of the multiple locations meets location criteria and the last location does not meet location criteria. ■ You use location awareness and no locations meet the criteria. ■ The location is renamed or changed in the policy. The client reverts to the default location when it receives the new policy. See "Changing a default location" on page 86.
Configure communications settings for locations	You can also configure the communication settings between a management server and the client on a location basis. See "Configuring communication settings for a location" on page 182.
Edit location properties	You can edit some location properties. See "Editing the name and description of a group's location" on page 87.

Table 5-1 Location awareness tasks that you can perform *(continued)*

Tasks	Description
Delete locations	You can delete any locations that are obsolete or no longer useful in your network. See "Deleting a group's location" on page 88.

About planning locations

Before you add locations to a group, you must consider the types of security policies that you need in your environment. You also must determine the criteria that define each location.

See "Using location awareness with groups" on page 79.

See "How you can structure groups" on page 55.

You should consider the following questions:

- From which locations are users connecting?
  Consider which locations need to be created and how to label each one. For example, users may connect at the office, from home, from a customer site, or from another remote site such as a hotel during travel. Additional qualified locations may be required at a large site.
- Should location awareness be set up for each location?
- How do you want to identify the location if using location awareness?
  You can identify the location based on IP addresses, WINS, DHCP, or DNS server addresses, network connections, and other criteria.
- If you identify the location by network connection, what type of connection is it?
  For example, the network connection may be a connection to the Symantec Endpoint Protection Manager, dial-up networking, or a particular brand of VPN server.
- Do you want clients connecting in this location to use a specific type of control, such as server control, mixed control, or client control?
- Do you want to do Host Integrity checks at each location? Or do you want to skip it at any time such as when not connected to the Symantec Endpoint Protection Manager?
- What applications and services should be allowed at each location?

- Do you want the location to use the same communication settings as the other locations in the group or to use different ones? You can set unique communication settings for one location.

Enabling location awareness for a client

To make the policies that are assigned to clients contingent on the client's connection location, you can enable location awareness for the client.

See "Using location awareness with groups" on page 79.

If you check **Remember the last location**, then when a client connects to the network, it is assigned the policy from the last-used location. If location awareness is enabled, then the client automatically switches to the appropriate policy after a few seconds. The policy that is associated with a specific location determines a client's network connection. If location awareness is disabled, the client can manually switch between any of the locations even when it is under server control. If a quarantine location is enabled, the client may switch to the quarantine policy after a few seconds.

If you uncheck **Remember the last location**, then when a client connects to the network, it is assigned the policy from the default location. The client cannot connect to the last-used location. If location awareness is enabled, then the client automatically switches to the appropriate policy after a few seconds. The policy that is associated with a specific location determines a client's network connection. If location awareness is disabled, the user can manually switch between any of the locations even when the client is under server control. If a quarantine location is enabled, the client may switch to the Quarantine Policy after a few seconds.

To enable location awareness for a client

1. In the console, click **Clients**.
2. On the **Clients** page, under **View Clients**, select the group for which you want to implement automatic switching of locations.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "*group name*"**.

   You can modify only the location-independent settings for those groups that have not inherited those policies and setting from a parent group.
4. Under **Location-independent Policies and Settings**, click **General Settings**.

5 In the **General Settings** dialog box, on the **General Settings** tab, under **Location Settings**, check **Remember the last location**.

By default, this option is enabled. The client is initially assigned to the policy that is associated with the location from which the client last connected to the network.

6 Check **Enable Location Awareness**.

By default, location awareness is enabled. The client is automatically assigned to the policy that is associated with the location from which the user tries to connect to the network.

7 Click **OK**.

Adding a location with a wizard

You can add a location to a group by using a wizard. Each location can have its own set of policies and settings. You set criteria (conditions) to trigger the clients to switch to a new location with different security settings whenever the conditions are met. The best security policies to apply typically depend on where the client is located when it connects to the network. When you have location awareness enabled, it ensures that the strictest security policy is assigned to a client when it is needed.

See "Using location awareness with groups" on page 79.

To add a location with a wizard

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

2 On the **Clients** page, under **View Clients**, select the group for which you want to add one or more locations.

3 On the **Policies** tab, uncheck **Inherit policies and settings from parent group "*group name*"**.

You can add locations only to groups that do not inherit policies from the parent group.

4 Under **Tasks**, click **Add Location**.

5 In the **Welcome to the Add Location Wizard** panel, click **Next**.

6 In the **Specify Location Name** panel, type a name and description for the new location, and click **Next**.

7 In the **Specify a Condition** panel, select any of the following conditions under which a client switches from one location to another:

No specific condition	Select this option so that the client can choose this location if multiple locations are available.
IP address range	Select this option so that the client can choose this location if its IP address is included in the specified range. You must specify both the start IP address and end IP address.
Subnet address and subnet mask	Select this option so that the client can choose this location if its subnet mask and subnet address are specified.
DNS server	Select this option so that the client can choose this location if it connects to the specified DNS server.
Client can resolve host name	Select this option so that the client can choose this location if it connects to the specified domain name and DNS resolve address.
Client can connect to management server	Select this option so that the client can choose this location if it connects to the specified management server.
Network connection type	Select this option so that the client can choose this location if it connects to the specified type of networking connection. The client switches to this location when using any of the following connections: ■ Any networking ■ Dial-up networking ■ Ethernet ■ Wireless ■ Check Point VPN-1 ■ Cisco VPN ■ Microsoft PPTP VPN ■ Juniper NetScreen VPN ■ Nortel Contivity VPN ■ SafeNet SoftRemote VPN ■ Aventail SSL VPN ■ Juniper SSL VPN

8 Click **Next**.

9 In the **Add Location Wizard Complete** panel, click **Finish**.

Adding a location without a wizard

You can add a location with its associated policies and settings to a group without the use of a wizard.

See "Using location awareness with groups" on page 79.

See "Adding a location with a wizard" on page 84.

To add a location without a wizard

1. In the console, click **Clients**.
2. In the **Clients** page, under **View Clients**, select the group for which you want to add one or more locations.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "*group name*"**.

   You can only add locations to groups that do not inherit policies from a higher group.
4. In the **Client** page, under **Tasks**, click **Manage Locations**.
5. In the **Manage Locations** dialog box, under Locations, click **Add**.
6. In the **Add Location** dialog box, type the name and description of the new location, and then click **OK**.
7. In the **Manage Locations** dialog box, next to **Switch to this location when**, click **Add**.
8. In the **Specify Location Criteria** dialog box, from the **Type** list, select and define a condition.

   A client computer switches to the location if the computer has the specified condition.
9. Click **OK**.
10. To add additional conditions, next to Switch to this location when, click **Add**, and then select either Criteria with AND relationship or Criteria with OR relationship.
11. Repeat steps 8 through 9.
12. Click **OK**.

Changing a default location

When the Symantec Endpoint Protection Manager is initially installed, only one location, called Default, exists. At that time, every group's default location is

Default. Every group must have a default location. When you create a new group, the Symantec Endpoint Protection Manager console automatically makes its default location Default.

See "Using location awareness with groups" on page 79.

You can specify another location to be the default location for a group after you add other locations. You may prefer to designate a location like Home or Road as the default location.

A group's default location is used if one of the following cases occurs:

- One of the multiple locations meets location criteria and the last location does not meet location criteria.
- You use location awareness and no locations meet the criteria.
- The location is renamed or changed in the policy. The client reverts to the default location when it receives the new policy.

To change a default location

1. In the console, click **Clients**.
2. On the **Clients** page, under **View Clients,** click the group to which you want to assign a different default location.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "*group name*"**.
4. Under **Tasks**, click **Manage Locations**.
5. In the **Manage Locations** dialog box, under **Locations**, select the location that you want to be the default location.
6. Under **Description**, check **Set this location as the default location in case of conflict**.

   The Default location is always the default location until you assign another one to the group.
7. Click **OK**.

Editing the name and description of a group's location

You can edit the name and description of a location at the group level.

See "Using location awareness with groups" on page 79.

To edit the name and description of a group's location

1. In the console, click **Clients**.
2. On the **Clients** pane, under **View Clients**, click the group whose name and description you want to edit.
3. On the **Policies** tab, in the **Tasks** pane, click **Manage Locations**.
4. In the **Location name** text box, edit the location name.
5. In the **Description** text box, edit the location description.
6. Click **OK**.

Deleting a group's location

You may need to delete a group's location because it no longer applies.

See "Using location awareness with groups" on page 79.

To delete a location

1. In the console, click **Clients**.
2. On the **Clients** page, under **View Clients**, select the group that contains the location you want to delete.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "*group name*"**.

   You can delete locations only from the groups that do not inherit policies from their parent groups.
4. On the **Clients** page, under **Tasks**, click **Manage Locations**.
5. In the **Manage Locations** dialog box, under **Locations**, select the location that you want to delete, and then click **Delete**.

   You cannot delete the location that is set as the default location.
6. In the **Delete Condition** dialog box, click **Yes**.

Chapter 6

Working with policies

This chapter includes the following topics:

- Configuring push mode or pull mode to update client policies and content
- Viewing the policy serial number
- Performing a manual policy update to check the policy serial number
- Monitoring the applications and services that run on client computers
- Configuring the management server to collect information about the applications that the client computers run
- Searching for information about the applications that the computers run

Using policies to manage your network security

You can use different types of security policies to manage your network security. Many policies are automatically created during the installation. You can use default policies or you can customize policies to suit your specific environment.

Note: A default policy is created during the initial installation for all types of policies except centralized exceptions.

Table 6-1 describes the different types of policies.

Table 6-1 Symantec Endpoint Protection Manager policies

Policy name	Description
Antivirus and Antispyware	Defines the antivirus and antispyware threat scan settings, including how detected processes are handled.
Firewall	Defines the firewall rules that allow and block traffic, and specifies settings for smart traffic filtering, traffic, and peer-to-peer authentication.
Intrusion Prevention	Defines the exceptions to the intrusion prevention signatures and specifies intrusion prevention settings, such as Active Response.
Host Integrity	Helps define, restore, and enforce the security of clients to keep enterprise networks and data secure.
Application and Device Control	Protects a system's resources from applications and manages the peripheral devices that can attach to computers.

Table 6-1 Symantec Endpoint Protection Manager policies *(continued)*

Policy name	Description
LiveUpdate	Specifies the computers that clients contact to check for updates. Also specifies the schedule that defines how often clients check for updates.
Centralized Exceptions	Specifies the exceptions to the particular policy features that you want to apply. There is no default policy.

You can perform a number of different tasks that are common to all types of policies.

Table 6-2 Tasks common to all policies

Task	Description
Add a policy	If you do not want to use one of the default policies, you can add a new policy. You can add shared policies or non-shared policies. **Note:** If you add or edit shared policies in the Policies page, you must also assign the policies to a group or location. Otherwise those policies are not effective. See "Adding a shared policy" on page 94. See "Adding a new non-shared policy in the Clients page" on page 95. See "Adding a new non-shared policy from an existing policy in the Clients page" on page 96. See "Adding a new non-shared policy from a previously exported policy file in the Clients page" on page 97.
Edit a policy	If you do not want to change the settings in a policy, you can edit it. See "Editing a policy" on page 97.
Assign a policy	To put a policy into use, you must assign it to one or more groups or locations. See "Assigning a shared policy" on page 98.

Table 6-2 Tasks common to all policies *(continued)*

Task	Description
Update the policies on clients	Based on the available bandwidth, you can configure a client to use push mode or pull mode as its update method. See "About updating policies on the clients" on page 108. See "Configuring push mode or pull mode to update client policies and content" on page 109.
Replace a policy	You can replace a shared policy with another shared policy. You can replace the shared policy in either all locations or for one location. See "Replacing a policy" on page 105.
Copy and paste a policy	Instead of adding a new policy, you may want to copy an existing policy to use as the basis for the new policy. See "About copying policies" on page 103. See "Copying and pasting a group policy" on page 105. See "Pasting a policy" on page 104. See "Copying a shared or non-shared policy in the Clients page" on page 104. See "Copying a shared policy in the Policy page" on page 103.
Import a policy	You can import a shared or non-shared policy and apply it to a group or to a specific location. See "Importing a policy" on page 102.
Export a policy	You can export an existing policy if you want to use at a different site. See "Exporting a policy" on page 101.

Table 6-2 Tasks common to all policies *(continued)*

Task	Description
Convert a shared policy to a non-shared policy	You can copy the content of a shared policy and create a non-shared policy from that content. A copy enables you to change the content of a shared policy in one location and not in all other locations. The copy overrides the existing non-shared policy. See "Converting a copy of a shared policy to a non-shared policy" on page 107. You can convert a shared policy to a non-shared policy if the policy no longer applies to all the groups or all the locations. When you finish the conversion, the converted policy with its new name appears under Location-specific Policies and Settings. See "Copying a shared policy to convert it to a non-shared policy" on page 107.
Withdraw a policy	If you do not want to delete a policy, but you no longer want to use it, you can withdraw it. You can withdraw any policy except an Antivirus and Antispyware Policy and a LiveUpdate Settings Policy. See "Withdrawing a policy" on page 99.
Delete a policy	If a policy is not longer useful, you can delete it. See "Deleting a policy" on page 100.

About shared and non-shared policies

Policies can be either shared or non-shared. A shared policy applies to any group and location. If you create shared policies, you can easily edit and replace a policy in all groups and locations that use it. You can have multiple shared policies.

You can apply shared policies at the My Company group level or a lower group level and subgroups can inherit policies.

A non-shared policy applies to a specific location in a group. You can only have one policy per location. You may need a specialized policy for a particular location that already exists. In that case, you can create a policy that is unique to a location.

You can apply one policy to a group or location or you can apply separate security policies to each location in a group. For example, take a group that has been assigned multiple locations. Users may need to connect to an enterprise network

by using different locations when in the office or when at home. You may need to apply a different policy with its own set of rules and settings to each location.

You apply a separate policy to each group of users or computers. Remote users typically use DSL and ISDN for which you may need a VPN connection. Other remote users may want to dial up when they connect to the enterprise network. Employees who work in the office typically use an Ethernet connection. However, the sales and marketing groups may also use wireless connections. Each of these groups may need its own Firewall policy for the locations from which they connect to the enterprise network.

You may want to implement a restrictive policy regarding the installation of non-certified applications on most employee workstations to protect the enterprise network from attacks. Your IT group may require access to additional applications. Therefore, the IT group may need a less restrictive security policy than typical employees. In this case, you can create a different Firewall policy for the IT group.

When you create a new policy, you start from the default rules and security settings, then edit the policy to customize them.

See "Using policies to manage your network security" on page 90.

About adding policies

You can add a policy as a shared policy or a non-shared policy.

You typically add any policy that groups and locations share in the Policies page on the Policies tab. However, you add any policy that is not shared between groups and that applies only to a specific location in the Clients page.

If you decide to add a policy in the Clients page, you can add a new policy by using any of the following methods:

- Base a new policy on an existing policy.
- Create a new policy.
- Import a policy from a previously exported policy.

See "Adding a shared policy" on page 94.

See "Using policies to manage your network security" on page 90.

Adding a shared policy

You typically add a shared policy in the Policies page instead of the Clients page. Locations as well as groups can share the same policy. You must assign the shared policy after you finish adding it.

You can add a non-shared policy from the Clients page.

See "Using policies to manage your network security" on page 90.

To add a shared policy in the Policies page

1. In the console, click **Policies**.
2. Under View Policies, select any of the policy types.
3. Under Tasks, click **Add a** *policy type* **Policy**.
4. On the *policy type* Policy page, in the Overview pane, type the name and description of the policy.
5. If not already checked, check **Enable this policy**.
6. In the Overview pane, select one of the following views:

Tree View	Any policies that have been assigned to groups and locations are represented as icons.
List View	Any policies that have been assigned to groups and locations are represented in a list.

7. To configure the policy, under View Policies, click a policy type, such as Antivirus and Antispyware Protection.
8. When you are done with the configuration of the policy, click **OK**.
9. In the Assign Policy dialog box, do one of the following tasks:
   - To assign the policy to a group or location now, click **Yes**, and then go to step 10.
   - To assign the policy to a group or a location later, click **No**.
     See "Assigning a shared policy" on page 98.

   You must assign the policy to a group or location or the client computers do not receive the policy.
10. In the Assign policy type Policy dialog box, check the groups and locations to which you want to apply the policy.
11. Click **Assign**.
12. To confirm, click **Yes**.

Adding a new non-shared policy in the Clients page

If you create a non-shared policy in the Clients page, the policy applies only to a specific location.

To add a new non-shared policy in the Clients page

1. In the Add Policy for *location name* wizard, select the policy type that you want to add, and then click **Next**.
2. Click **Create a new policy**, and then click **Next**.
3. In the *policy type* Policy Overview pane, type the name and description of the policy.
4. To configure the policy, under View Policies, click any of the following types of policies:

Antivirus and Antispyware	See "About working with Antivirus and Antispyware Policies" on page 393.
Firewall	See "About working with Firewall Policies" on page 462.
Intrusion Prevention	See "About working with Intrusion Prevention Policies" on page 486.
Application and Device Control	See "About working with Application and Device Control " on page 543.
Host Integrity	
LiveUpdate	See "About LiveUpdate Policies" on page 142.
Centralized Exceptions	See "About working with Centralized Exceptions Policies" on page 576.

Adding a new non-shared policy from an existing policy in the Clients page

You can add a new non-shared policy from an existing policy in the Clients page.

See "Using policies to manage your network security" on page 90.

To add a new non-shared policy from an existing policy in the Clients page

1. In the Add Policy for *location name* wizard, select the policy type that you want to add, and then click **Next**.
2. Click **Use an existing shared policy**, and then click **Next**.
3. In the Add Policy dialog box, select an existing policy from the Policy drop-down list.
4. Click **OK**.

Adding a new non-shared policy from a previously exported policy file in the Clients page

You can add a new non-shared policy from a previously exported policy file in the Clients page.

See "Using policies to manage your network security" on page 90.

To add a new non-shared policy from a previously exported policy file in the Clients page

1. In the Add Policy for *location name* wizard, select the policy type that you want to add, and then click **Next**.
2. Click **Import a policy from a policy file**, and then click **Next**.
3. In the Import Policy dialog box, browse to locate the .dat file that was previously exported.
4. Click **Import**.

Editing a policy

You can edit shared policies both on the Policies tab in the Policies page as well as in the Client page. However, you can edit only non-shared policies in the Clients page.

See "Using policies to manage your network security" on page 90.

Locations as well as groups can share the same policy. You must assign a shared policy after you edit it.

You can edit both non-shared as well as shared policies in the Clients page.

To edit a shared policy in the Policies page

1. In the console, click **Policies**.
2. On the Policies page, under View Policies, click the policy type.
3. In the *policy type* Policies pane, click the specific policy that you want to edit
4. Under Tasks, click **Edit the Policy**.
5. In the *policy type* Policy Overview pane, edit the name and description of the policy, if necessary.
6. To edit the policy, click any of the *policy type* Policy pages for the policies.

To edit a non-shared or a shared policy in the Clients page

1. In the console, click **Clients**.
2. On the Clients page, under View Clients, select the group for which you want to edit a policy.
3. On the Policies tab, uncheck **Inherit policies and settings from parent group "*group name*"**.

   You must disable inheritance for this group. If you do not uncheck inheritance, you cannot edit a policy.
4. Under Location-specific Policies and Settings, scroll to find the name of the location whose policy you want to edit.
5. Locate the specific policy for the location that you want to edit.
6. To the right of the selected policy, click **Tasks**, and then click **Edit Policy**.
7. Do one of the following tasks:
   - To edit a non-shared policy, go to step 8.
   - To edit a shared policy, in the Edit Policy dialog box, click **Edit Shared** to edit the policy in all locations.
8. You can click a link for the type of policy that you want to edit.

Assigning a shared policy

After you create a shared policy in the Policies page, you must assign it to one or more groups and one or more locations. Unassigned policies are not downloaded to the client computers in groups and locations. If you do not assign the policy when you add the policy, you can assign it to groups and locations later. You can also reassign a policy to a different group or location.

See "Using policies to manage your network security" on page 90.

To assign a shared policy

1. Create a shared policy.

   See "Adding a shared policy" on page 94.
2. On the Policies page, under View Policies, select the policy type that you want to assign.
3. In the *policy type* Policies pane, select the specific policy that you want to assign.
4. On the Policies page, under Tasks, click **Assign the Policy**.

5 In the Assign *policy type* Policy dialog box, check the groups and locations to which you want to assign the policy.

6 Click **Assign**.

7 Click **Yes** to confirm that you want to assign the policy.

Withdrawing a policy

You may want to withdraw a policy from a group or a location under certain circumstances. For example, a specific group may have experienced problems after you introduced a new policy. If you withdraw a policy, it is automatically withdrawn from the groups and locations that you assigned it to. However, the policy remains in the database.

See "Using policies to manage your network security" on page 90.

You can withdraw all policies in the Policies page except for the following policies:

- Antivirus and Antispyware
- LiveUpdate

Note: You must withdraw a policy from all groups and locations before you can delete it. You cannot withdraw an Antivirus and Antispyware Policy or a LiveUpdate Policy from a location or group. You can only replace them with another Antivirus and Antispyware Policy or a LiveUpdate Policy.

To withdraw a shared policy in the Policies page

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

2 On the Policies page, under View Policies, click the type of policy that you want to withdraw.

3 In the *policy type* Policies pane, click the specific policy that you want to withdraw.

4 On the Policies page, under Tasks, click **Withdraw the Policy**.

5 In the Withdraw Policy dialog box, check the groups and locations from which you want to withdraw the policy.

6 Click **Withdraw**.

7 When you are prompted to confirm the withdrawal of the policy from the groups and locations, click **Yes**.

To withdraw a shared or non-shared policy in the Clients page

1. In the console, click **Clients**.
2. On the Clients page, under View Clients, select the group for which you want to withdraw a policy.
3. On the Policies tab, uncheck **Inherit policies and settings from parent group "*group name*"**.

   You must disable inheritance for this group. If you do not uncheck inheritance, you cannot withdraw a policy.
4. Under Location-specific Policies and Settings, scroll to find the name of the location for which you want to withdraw a policy.
5. Locate the policy for the location that you want to withdraw.
6. Click **Tasks**, and then click **Withdraw Policy**.
7. In the Withdraw Policy dialog box, click **Yes**.

Deleting a policy

You may need to delete a policy that applies to groups and locations. For example, corporate guidelines may change that require the implementation of different policies. As new corporate groups are added, you may need to delete old groups and its associated policies.

See "Using policies to manage your network security" on page 90.

You may want to delete a shared policy or a non-shared policy. As new groups and locations are added, you may need to delete old policies.

To delete a non-shared policy, you withdraw and delete it by using the same command.

Note: You must first withdraw a policy that has been assigned to a group or location before you can delete the policy. You cannot withdraw an Antivirus and Antispyware Policy or a LiveUpdate Policy. Instead, you must first replace it with another Antispyware Policy or a LiveUpdate Policy. Then you can delete the original Antispyware Policy or a LiveUpdate Policy. You must have at least one Antispyware Policy and one LiveUpdate Policy for each group and each location.

To delete a shared policy in the Policy page

1. In the console, click **Policies**.
2. In the Policies page, under View Policies, select the type of policy that you want to delete.

   The policy may or may not have been assigned to one or more groups and one or more locations.
3. In the *policy type* Policies pane, click the specific policy that you want to delete.
4. In the Policies page, under Tasks, click **Delete the Policy**.
5. When you are prompted to confirm that you want to delete the policy that you selected, click **Yes**.

To delete a non-shared policy in the Clients page

1. In the console, click **Clients**.
2. In the Clients page, under View Clients, select the group for which you want to delete a policy.
3. On the Policies tab, uncheck **Inherit policies and settings from parent group "***group name***"**.

   You must disable inheritance for this group. If you do not uncheck inheritance, you cannot delete a policy.
4. Under Location-specific Policies and Settings, scroll to find the name of the location whose policy you want to delete.
5. Locate the specific policy for the location that you want to delete.
6. To the right of the selected policy, click **Tasks**, and then click **Withdraw Policy**.

   When you withdraw the policy, you delete it at the same time. You cannot delete an Antivirus and Antispyware Policy or a LiveUpdate Policy from a location. You can only replace it with another policy.
7. Click **Yes**.

Exporting a policy

You can export existing policies to a .dat file. For example, you may want to export a policy for use at a different site. At the other site, you have to import the policy by using the .dat file from the original site. All the settings that are associated with the policy are automatically exported.

See "Using policies to manage your network security" on page 90.

You can export a shared or non-shared policy.

To export a shared policy in the Policies page

1. In the console, click **Policies**.
2. On the Policies page, under View Policies, click the type of policy that you want to export.
3. In the *policy type* Policies pane, click the specific policy that you want to export.
4. In the Policies page, under Tasks, click **Export the Policy**.
5. In the Export Policy dialog box, locate the folder where you want to export the policy file to, and then click **Export**.

To export a shared or non-shared policy in the Clients page

1. In the console, click **Clients**.
2. On the Clients page, under View Clients, select the group for which you want to export a policy.
3. On the Policies tab, uncheck **Inherit policies and settings from parent group "***group name***"**.

   You must disable inheritance for this group. If you do not uncheck inheritance, you cannot export a policy.
4. Under Location-specific Policies and Settings, scroll to find the name of the location whose policy you want to export.
5. Locate the specific policy for the location that you want to export.
6. To the right of the policy, click **Tasks**, and then click **Export Policy**.
7. In the Export Policy dialog box, browse for the folder into which you want to export the policy.
8. In the Export Policy dialog box, click **Export**.

Importing a policy

You can import a policy file and apply it to a group or only to a location. The format of the import file is .dat.

You can import a shared or non-shared policy for a specific location in the Clients page.

See "Adding a new non-shared policy from a previously exported policy file in the Clients page" on page 97.

See "Using policies to manage your network security" on page 90.

To import a policy

1. In the console, click **Policies**.
2. On the Policies page, under View Policies, click the type of policy that you want to import.
3. In the *policy type* Policies pane, click the policy that you want to import.
4. On the Policies page, under Tasks, click **Import a** *policy type* **Policy**.
5. In the Import Policy dialog box, browse to the policy file that you want to import, and then click **Import**.

About copying policies

You may want to copy any of the policies before you customize them. After you copy a policy, you must paste it.

See "Pasting a policy" on page 104.

Copying a shared policy in the Policy page

You can copy a shared policy in the Policy page.

You can also copy a shared policy on the Clients page.

See "Copying a shared or non-shared policy in the Clients page" on page 104.

To copy a shared policy in the Policy page

1. In the console, click **Policies**.
2. On the Policies page, under View Policies, click the type of policy that you want to copy.
3. In the *policy type* Policies pane, click the specific policy that you want to copy.
4. On the Policies page, under Tasks, click **Copy the Policy**.
5. In the Copy Policy dialog box, check **Do not show this message again**.

   You check this option only if you no longer want to be notified about this process. The message states that the policy has been copied to the clipboard and is ready to be pasted.
6. Click **OK**.

Copying a shared or non-shared policy in the Clients page

You can copy a shared or non-shared policy in the Clients page. However, you must subsequently paste the policy in the Clients page.

You can also copy shared policies in the Policy page.

See "Copying a shared policy in the Policy page" on page 103.

To copy a shared or non-shared policy in the Clients page

1. In the console, click **Clients**.
2. On the **Clients** page, under **View Clients**, select the group for which you want to copy a policy.
3. On the **Policies** tab, under **Location-specific Policies and Settings**, scroll to find the name of the location from which you want to copy a policy.
4. Locate the specific policy for the location that you want to copy.
5. To the right of the policy, click **Tasks**, and then click **Copy**.
6. Click **OK**.

Pasting a policy

You must have already copied a policy before you can paste it.

For shared policies, when you paste a policy, the policy appears in the right-hand pane. The words "Copy of" are added to the beginning of the name of the policy to distinguish it as a copy. You can then edit the copied policy's name.

See "About copying policies" on page 103.

To paste a shared policy in the Policy page

1. In the console, click **Policies**.
2. On the Policies page, under View Policies, click the type of policy that you want to paste.
3. In the *policy type* Policies pane, click the specific policy that you want to paste.
4. On the Policies page, under Tasks, click **Paste a Policy**.

To paste a shared or non-shared policy in the Clients page

1. In the console, click **Clients**.
2. On the Clients page, under View Clients, select the group for which you want to paste a policy.

3 On the Policies tab, uncheck **Inherit policies and settings from parent group "***group name***"**.

You must disable inheritance for this group. If you do not uncheck inheritance, you cannot paste a policy.

4 Under Location-specific Policies and Settings, scroll to find the name of the location whose policy you want to paste.

5 Locate the specific policy for the location that you want to paste.

6 To the right of the policy, click **Tasks**, and then click **Paste**.

7 When you are prompted to overwrite the existing policy, click **Yes**.

Copying and pasting a group policy

You can copy the group settings, locations, and policies that are assigned to one group and paste them onto another group. The newly copied settings, locations, and policies override the settings in the paste group's existing policies.

See "Using policies to manage your network security" on page 90.

To copy and paste a group policy

1 In the console, click **Clients**, and then click the **Policies** tab.

2 Click the group from which you want to copy the policies.

3 Under Tasks, click **Copy Group Policy**.

4 Click the group to which you want to copy the policies.

5 Under Tasks, click **Paste Group Policy**.

6 In the confirmation dialog box, click **Yes**.

Replacing a policy

You may want to replace one shared policy with another shared policy. You can replace the shared policy in either all locations or for one location.

When you replace a policy for all locations, the management server replaces the policy only for the locations that have it. For example, suppose the Sales group uses the Sales policy for three of its four locations. If you replace the Sales policy with the Marketing policy, only those three locations receive the Marketing policy.

You may want a group of clients to use the same settings no matter what location they are in. In this case, you can replace a non-shared policy with a shared policy. You replace a non-shared policy with a shared policy for each location separately.

See "Using policies to manage your network security" on page 90.

To replace a shared policy for all locations

1. In the console, click **Policies**.
2. On the Policies page, under View Policies, click the type of policy that you want to replace.
3. In the *policy type* Policies pane, click the policy.
4. In the Policies page, under Tasks, click **Replace the Policy**.
5. In the Replace *policy type* Policy dialog box, in the New *policy type* Policy drop-down list, select the shared policy that replaces the old one.
6. Select the groups and locations for which you want to replace the existing policy.
7. Click **Replace**.
8. When you are prompted to confirm the replacement of the policy for the groups and locations, click **Yes**.

To replace a shared policy or non-shared policy for one location

1. In the console, click **Clients**.
2. In the Clients page, under View Clients, select the group for which you want to replace a policy.
3. On the Policies tab, uncheck **Inherit policies and settings from parent group "***group name***"**.

   You must disable inheritance for this group. If you do not uncheck inheritance, you cannot replace a policy.
4. Under Location-specific Policies and Settings, scroll to find the location that contains the policy.
5. Next to the policy that you want to replace, click **Tasks**, and then click **Replace Policy**.
6. In the Replace Policy dialog box, in the New policy drop-down list, select the replacement policy.
7. Click **OK**.

Copying a shared policy to convert it to a non-shared policy

You may want to convert an existing shared policy to a non-shared policy because the policy no longer applies to all the groups or all the locations that share the policy.

When you finish the conversion, the converted policy with its new name appears under **Location-specific Policies and Settings**.

To copy and convert a shared policy to a non-shared policy

1. In the console, click **Clients**.
2. In the **Clients** page, under **View Clients**, select the group for which you want to convert a policy.
3. In the pane that is associated with the group that you selected in the previous step, click **Policies**.
4. On the Policies tab, uncheck **Inherit policies and settings from parent group "***group name***"**.

   If you do not uncheck inheritance, you cannot export any policies.
5. Under **Location-specific Policies and Settings**, scroll to find the name of the location and the specific policy for the location that you want to convert.
6. Beside the specific policy, click **Tasks**, and then click **Convert to Non-shared Policy**.
7. In the **Overview** dialog box, edit the name and description of the policy.
8. Click **OK**.

Converting a copy of a shared policy to a non-shared policy

You can copy the content of a shared policy and create a non-shared policy from that content. A copy enables you to change the content of a shared policy in one location and not in all other locations. The copy overrides the existing non-shared policy.

To convert a copy of a shared policy to a non-shared policy

1. In the console, click **Clients**.
2. In the Clients page, under View Clients, select the group for which you want to replace a policy.

3 On the Policies tab, uncheck **Inherit policies and settings from parent group "*group name*"**.

You must disable inheritance for this group. If you do not uncheck inheritance, you cannot replace a policy.

4 Under Location-specific Policies and Settings, scroll to find the location that contains the policy.

5 Next to the policy that you want to replace, click **Tasks**, and then click **Edit Policy**.

6 In the Edit Policy dialog box, click **Create Non-Shared Policy From Copy**.

7 Edit the policy.

See "Editing a policy" on page 97.

8 When you are done with the configuration of the policy, click **OK**.

About updating policies on the clients

When you configure policies on the management server, you need to get the updated policies downloaded to the clients. In the console, you can configure clients to use either one of the following two update methods:

pull mode	The client connects to the manager periodically depending on the frequency of the heartbeat setting. The client checks the status of the management server when the client connects.
push mode	The client establishes a constant HTTP connection to the management server. Whenever a change occurs in the management server status, it notifies the client immediately.

In either mode, the client takes the corresponding action that is based on the change in the status of the management server. Because it requires a constant connection, push mode requires a large network bandwidth. Most of the time you should set up clients in pull mode.

See "Configuring push mode or pull mode to update client policies and content" on page 109.

A heartbeat is the frequency at which client computers upload data such as log entries and download policies. A heartbeat is a protocol that each client uses to communicate with the Symantec Endpoint Protection Manager. The first heartbeat occurs immediately after the client starts. The next heartbeat occurs at the heartbeat frequency that you set.

The heartbeat frequency is a key factor in the number of clients that each Symantec Endpoint Protection Manager can support. If you set a heartbeat frequency to 30 minutes or less, it limits the total number of clients that Symantec Endpoint Protection Manager can support. For deployments of 1,000 clients or more, you should set the heartbeat frequency to the maximum length of time that meets a company's security requirements. For example, if you want to update security policies and gather logs on a daily basis, then set the heartbeat frequency to 24 hours. Consult Symantec Professional Services and Symantec Enterprise Support to assess the proper configuration, hardware, and network architecture necessary for your network environment.

Configuring push mode or pull mode to update client policies and content

You can specify whether the management server pushes the policy down to the clients or that the clients pull the policy from the management server. The default setting is push mode. If you select pull mode, then by default, clients connect to the management server every 5 minutes, but you can change this default heartbeat interval.

See "About updating policies on the clients" on page 108.

You can set the mode for a group or for a location.

To configure push mode or pull mode for a group

1. In the console, click **Clients**.
2. On the **Clients** page, under **View Clients**, select the group for which you want to specify whether to push or pull policies.
3. On the **Clients** page, click the **Policies** tab.
4. On the **Policies** tab, uncheck **Inherit policies and setting from the parent group "***group name***"**.
5. Under **Location-independent Policies and Settings** pane, under **Settings**, click **Communications Settings**.
6. In the **Communications Settings for** *group name* dialog box, under **Download**, verify that **Download policies and content from the management server** is checked.
7. Do one of the following tasks:
   - Click **Push mode**.

- Click **Pull mode** and under Heartbeat Interval, set the number of minutes or hours.

8 Click **OK**.

To specify push or pull mode for a location

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

2 On the **Clients** page, under **View Clients**, select the group for which you want to specify whether to push or pull policies.

3 On the **Clients** page, click the **Policies** tab.

1 On the **Policies** tab, uncheck **Inherit policies and setting from the parent group "***group name***"**.

2 Under **Location-specific Policies and Settings**, under **Location-specific Policies** for the location you want to modify, expand **Location-specific Settings**.

3 Under **Location-specific Settings**, to the right of **Communications Settings**, click **Tasks** and uncheck **Use Group Communications Settings**.

4 To the right of **Communications Settings**, click **Local - Push** or (**Local - Pull**).

5 Do one of the following tasks:

- Click **Push mode**.
- Click **Pull mode** and under Heartbeat Interval, set the number of minutes or hours.

6 Click **OK**.

Viewing the policy serial number

You should check the policy serial number on the client to see if it matches the serial number that appears in the management console. If the client communicates with the management server and receives regular policy updates, the serial numbers should match.

If the policy serial numbers do not match, you can try to manually update the policies on the client computer and check the troubleshooting logs.

See "Performing a manual policy update to check the policy serial number" on page 111.

To view the policy serial number in the management console

1. On the management server, in the console, click **Clients**.
2. Under View Clients, select the relevant group, and then click **Details**.

   The policy serial number and the policy date appear at the bottom of the details list.

To view the policy serial number on the client

1. On the client computer, in the client, on the Help and Support menu, click **Troubleshooting**.
2. On the Management tab, look at the policy serial number.

   The serial number should match the serial number of the policy that the management server pushes to the client.

Performing a manual policy update to check the policy serial number

You can perform a manual policy update to check whether or not the client receives the latest policy update. If the client does not receive the update, there might be a problem with the client and server communication.

You can try a manual policy update by doing any of the following actions:

- In the client on the Help and Support menu, in the Troubleshooting dialog box, under Policy Profile, you can click **Update**. You can use this method if you want to perform a manual update on a particular client.
- For the clients that are configured for pull mode, the management server downloads policies to the client at regular intervals (heartbeat). You can change the heartbeat interval so that policies are downloaded to the client group more quickly. After the heartbeat interval, you can check to see if the policy serial numbers match. (For the clients that are configured for push mode, the clients receive any policy updates immediately.)

After you run a manual policy update, make sure that the policy serial number that appears in the client matches the serial number that appears in the management console.

See "Viewing the policy serial number" on page 110.

To perform a manual policy update

1. On the client, click **Help > Troubleshooting**
2. In the Troubleshooting dialog box, in the left column, select **Management**.
3. On the Management panel, under **Policy Profile**, click **Update**.

Monitoring the applications and services that run on client computers

The client monitors and collects information about the applications and the services that run on each computer. You can configure the client to collect the information in a list and send the list to the management server. The list of applications and their characteristics is called learned applications.

You can use this information to find out what applications your users run. You can also use the information when you need information about applications in the following areas:

- Firewall Policies
- Application and Device Control Policies
- TruScan proactive threat scans
- Host Integrity Policies
- Network application monitoring
- File fingerprint lists

You can perform several tasks to set up and use learned applications.

Table 6-3 Steps to monitor the applications

Steps	Description
Enable learned applications	Configure the management server to collect information about the applications that the client computers run. See "Configuring the management server to collect information about the applications that the client computers run" on page 113.

Table 6-3 Steps to monitor the applications *(continued)*

Steps	Description
Search for applications	You can use a query tool to search for the list of applications that the client computers run. You can search on application-based criteria or computer-based criteria. For example, you can find out the version of Internet Explorer that each client computer uses. See "Searching for information about the applications that the computers run" on page 115. You can save the results of an application search for review. See "Saving the results of an application search" on page 117.

Note: In some countries, it may not be permissible under local law to use the learned applications tool under certain circumstances, such as to gain application use information from a laptop when the employee logs on to your office network from home using a company laptop. Before your use of this tool, please confirm that use is permitted for your purposes in your jurisdiction. If it is not permitted, please follow instructions for disabling the tool.

Note: The client does not record information about the applications that Symantec Network Access Control clients run. The learned applications feature is not available on the console if you install Symantec Network Access Control only. If you integrate Symantec Network Access Control with Symantec Endpoint Protection, you can use the learned applications tool with Host Integrity Policies. You must install the Network Threat Protection module and the Application and Device Control module on the client for this feature to work.

Configuring the management server to collect information about the applications that the client computers run

You can enable learned applications for whole sites, for groups within a site, or for locations within a group. The learned applications feature is enabled by default for the site, group, and location. You first enable learned applications for each site, and then you optionally enable learned applications for specific groups and locations.

To enable learned applications, you must complete the following tasks:

- Enable learned applications for the site.
  You must enable the learned applications tool for a site to use the tool for a specific group or a location.
- Enable the clients to send learned applications to the management server by group or by location.

You can set up a notification to be sent to your email address when each client in a group or location runs an application.

See "Creating administrator notifications" on page 283.

You can set up learned applications for the management servers within a local site or within a remote site.

To enable learned applications for a site

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, do one of the following actions:
   - Click **Local Site (Site** *site name***)**.
   - Expand **Remote Sites,** and then click **(Site** *site name***)**.
3. Under Tasks, click **Edit Site Properties**.
4. In the Site Properties for *site name* dialog box, on the General tab, check **Keep track of every application that the clients run**.
5. Click **OK**.

After you have enabled a site to collect the lists of learned applications from the clients, you enable the clients to send the lists to the server by group or by location.

Note: You can modify this setting only for the subgroups that do not inherit their policies and settings from a parent group.

To send the learned applications list to the management server

1. In the console, click **Clients**.
2. Under View Clients, select a group.
3. On the Policies tab, click **Communications Settings**.
4. In the Communications Settings for *group name* dialog box, make sure **Learn applications that run on the client computers** is checked.
5. Click **OK**.

To send learned applications to the management server for a location

1. In the console, click **Clients**.
2. Under View Clients, select a group.
3. Under Location-specific Policies and Settings, select the location, and then expand **Location-specific Settings**.
4. To the right of Communications Settings, click **Tasks**, and then uncheck **Use Group Communications Settings**.

   Checking this setting enables you to create a location setting rather than a group setting.
5. Click **Tasks**, and then click **Edit Settings**.
6. In the Communications Settings for *location name* dialog box, check **Learn applications that run on the client computers**.
7. Click **OK**.

Searching for information about the applications that the computers run

After the management server receives the list of applications from the clients, you can query the details about the applications. For example, you can find all the client computers that use an unauthorized application. You can then create a firewall rule to block the application on the client computer. Or you may want to upgrade all the client computers to use the most current version of Microsoft Word.

You can search for an application in the following ways:

- By application.
  You can limit the search to specific applications or application details such as its name, file fingerprint, path, size, version, or last modified time.
- By client or client computer.
  You can search for the applications that either a specific user runs or a specific computer runs. For example, you can search on the computer's IP address.

You can also search for application names to add to a firewall rule, directly within the Firewall Policy.

See "Adding applications to a rule" on page 509.

Note: The information in the **Search** box is not collected until you enable the feature that keeps track of all the applications that clients run. You can go to the **Admin** page **Site Properties for *site name*** dialog box **General** tab to enable this feature.

To search for information about the applications that the computers run

1. In the console, click **Policies**.
2. On the **Policies** page, under **Tasks**, click **Search for Applications**.
3. In the **Search for Applications** dialog box, to the right of the **Search for applications in** field, click **Browse**.
4. In the **Select Group or Location** dialog box, select a group of clients for which you want to view the applications, and then click **OK**.

   You can specify only one group at a time.
5. Make sure that **Search subgroups** is checked.
6. Do one of the following actions:
   - To search by user or computer information, click **Based on client/computer information**.
   - To search by application, click **Based on applications**.
7. Click the empty cell under **Search Field**, and then select the search criterion from the list.

   The Search Field cell displays the criteria for the option that you selected. For details about these criteria, click **Help**.
8. Click the empty cell under Comparison Operator, and then select one of the operators.
9. Click the empty cell under Value, and then select or type a value.

   The Value cell may provide a format or a value from the drop-down list, depending on the criterion you selected in the Search Field cell.
10. To add an additional search criterion, click the second row, and then enter information in the Search Field, Comparison Operator, and Value cells.

    If you enter more than one row of search criteria, the query tries to match all conditions.
11. Click **Search**.
12. In the Query Results table, do any of the following tasks:
    - Click the scroll arrows to view additional rows and columns.

- Click **Previous** and **Next** to see additional screens of information.
- Select a row, and then click **View Details** to see additional information about the application.

The results are not saved unless you export them to a file.

13 To remove the query results, click **Clear All**.

14 Click **Close**.

Saving the results of an application search

After you run the query, you can save the results in a text or a comma delimited file. The query tool exports all the results of the query, rather than a selected row.

To save the results of an application search

1 Search for the details about an application or a client computer.

See "Searching for information about the applications that the computers run" on page 115.

2 In the Search for Applications dialog box, under Query Results, click **Export**.

3 In the Export Results dialog box, type the number for the page that contains the application details and client computer details that you want to export.

4 Select or type the path name and the file name where you want to export the file, and then click **Export**.

5 To confirm, click **OK**.

6 If you are finished searching for applications, click **Close**.

Chapter 7

Working with client installation packages

This chapter includes the following topics:

Using client installation packages

To manage computers with Symantec Endpoint Protection Manager, you must export at least one client installation package to a management server in the site. After you export the client installation package, you then install the files in the package onto client computers. You can export packages for Symantec-managed clients, third-party managed clients, and unmanaged clients.

You can use the console to export these packages as a single executable file or as a series of files in a directory. The method that you choose depends on your deployment method and whether you want to upgrade client software in groups from the console. The single executable is available for third-party installation tools and for potential bandwidth conservation. Typically, if you use Active

Directory Group Policy Object, you would not choose to export to a single executable file.

During the export process, you select either the 32-bit installation packages or the 64-bit installation packages that are provided by default. You then optionally select the specific client protection technologies to install if you do not want to install all components. You can also specify how the installation interacts with end users. Finally, you can install the exported files (a package) to computers one at a time, or deploy the exported files to multiple computers simultaneously.

For client installation deployment options, refer to the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* on the product disc.

Symantec occasionally provides updated packages of installation files. When client software is installed on client computers, you can automatically update the client software on all clients in a group with the auto-upgrade feature. You do not need to redeploy software with installation deployment tools.

Table 7-1 Client installation package-related tasks

Task	Description
Configure client installation packages	You can select specific client protection technologies to install and you can specify how the installation interacts with end users. See "Configuring client installation package options" on page 121.
Export client installation packages	You can export packages for Symantec-managed clients, third-party managed clients, and unmanaged clients. See "Exporting client installation packages" on page 123.
Deploy client installation packages by using the Find Unmanaged Computers feature	You can deploy client installation packages to computers that do not run the client software by using the Find Unmanaged Computers feature. See "Deploying client software with Find Unmanaged Computers" on page 125.

Table 7-1 Client installation package-related tasks *(continued)*

Task	Description
Add client installation package updates	When you receive client installation package updates from Symantec, you add them to the site database. You add them to the site database to make them available for distribution from Symantec Endpoint Protection Manager. You can optionally export the packages during this procedure to make the package available for deployment to computers that do not run the client software. See "Adding client installation package updates" on page 126.
Upgrade clients in one or more groups	You can install the exported packages to computers one at a time, or deploy the exported files to multiple computers simultaneously. See "About adding client installation package updates and upgrading clients" on page 126. See "Upgrading clients in one or more groups" on page 127.
Delete client installation packages	You can delete older client installation packages to save disk space. See "Deleting upgrade packages" on page 128.

Configuring client installation package options

When you export client installation packages, you can select which client components are installed and how. You can optionally prompt users to send information about themselves, which then appears as properties for the computers in the console.

See "Using client installation packages" on page 119.

Configuring client installation package features

Installation features are the client components that are available for installation. For example, if you create Symantec Endpoint Protection packages, you can select to install the antivirus features and the firewall features. Or, you can select to install only the antivirus feature.

You must name each set of selections. You then select a named set of features when you export 32-bit client software packages and 64-bit client software packages.

See "Using client installation packages" on page 119.

To configure client installation package features

1. In the console, click **Admin**, and then click **Install Packages**.
2. Under View Install Packages, click **Client Install Feature Sets**.
3. Under Tasks, click **Add Client Install Feature Set**.
4. In the Add Client Install Feature Set dialog box, in the Name box, type a name.
5. In the Description box, type a description of the client installation feature set.
6. For details about setting other options in this dialog box, click **Help**.
7. Click **OK**.

Configuring client installation package settings

Installation settings affect how client installation software is installed on client computers. You must name each set of selections. You then select a named set of package settings when you export 32-bit client software packages and 64-bit client software packages.

See "Using client installation packages" on page 119.

To configure client installation package settings

1. On the Admin tab, in the lower-left pane, click **Install Packages**.
2. Under View Install Packages, click **Client Install Settings**.
3. Under Tasks, click **Add Client Install Settings**.
4. In the Client Install Settings dialog box, in the Name box, type a name.
5. For details about setting other options in this dialog box, click **Help**.
6. Click **OK**.

Collecting user information

You can prompt users on the client computers to type information about themselves during the client software installation process or during policy updates. You can collect information such as the employee's mobile phone number, job title, and email address. After you collect this information, you must maintain and update it manually.

Note: After you enable the message to appear on the client computer for the first time, and the user responds with the requested information, the message does not appear again. Even if you edit any of the fields or disable and reenable the message, the client does not display a new message. However, the user can edit the information at any time, and the management server retrieves that information.

See "Using client installation packages" on page 119.

To collect user information

1. In the console, click **Admin**, and then click **Install Packages**.
2. Under **View Install Packages**, click **Client Install Packages**.
3. In the **Client Install Packages** pane, click the package for which you want to collect user information.
4. Under **Tasks**, click **Set User Information Collection**.
5. In the **Set User Information Collection** dialog box, check **Collect User Information**.
6. In the **Pop-up Message** text box, type the message that you want users to read when they are prompted for information.
7. If you want the user to have the ability to postpone user information collection, check **Enable Remind Me Later**, and then set a time in minutes.
8. Under **Select the fields that will be displayed for the user to provide input**, choose the type of information to collect, and then click **Add**.

   You can select one or more fields simultaneously by pressing the Shift key or the Control key.
9. In the Optional column, check the check box next to any fields that you want to define as optional for the user to complete.
10. Click **OK**.

Exporting client installation packages

When you export client software packages, you create client installation files for deployment. When you export packages, you must browse to a directory to contain the exported packages. If you specify a directory that does not exist, it is automatically created for you. The export process creates descriptively named subdirectories in this directory and places the installation files in these subdirectories.

For example, if you create an installation package for a group named **My Group** beneath **My Company**, a directory named **My Company_My Group** is created. This directory contains the exported installation package.

Note: This naming convention does not make a distinction between client installation packages for Symantec Endpoint Protection and Symantec Network Access Control. The exported package name for a single executable is Setup.exe for both Symantec Endpoint Protection and Symantec Network Access Control. Therefore, be sure to create a directory structure that lets you distinguish between Symantec Endpoint Protection and Symantec Network Access Control installation files.

You have one important decision to make when you export packages. You must decide whether to create an installation package for managed clients or unmanaged clients. If you create a package for managed clients, you can manage them with the Symantec Endpoint Protection Manager console. If you create a package for unmanaged clients, you cannot manage them from the console.

Note: If you export client installation packages from a remote console, the packages are created on the computer from which you run the remote console. Furthermore, if you use multiple domains, you must export the packages for each domain, or they do not appear as available for the domain groups.

After you export one or more installation package of files, you deploy the installation files on client computers.

See "Using client installation packages" on page 119.

For details about client software installation, see the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* on the product disk.

To export client installation packages

1. In the console, click **Admin**, and then click **Install Packages**.
2. Under **View Install Packages**, click **Client Install Packages**.
3. In the **Client Install Packages** pane, under **Package Name**, right-click the package to export and then click **Export**.

4 In the **Export Package** dialog box, beside the **Export folder** text box, browse to and select the directory to contain the exported package, and then click **OK**.

   Directories with double-byte or high-ASCII characters are not supported and are blocked.

5 In the **Export Package** dialog box, set the other options according to your installation goals.

6 For details about setting other options in this dialog box, click **Help**.

7 Click **OK**.

Deploying client software with Find Unmanaged Computers

You can deploy client software by using Find Unmanaged Computers in the Symantec Endpoint Protection Manager console. The utility lets you discover the client computers that do not run client software and then install the client software on those computers.

Note: You can use this utility only to discover Windows client computers. Mac client computers are listed in the utility as Unknown, and Mac client install packages must be deployed separately.

Warning: This utility detects and displays a variety of networking devices in the unknown computers tab. For example, this utility detects router interfaces and places them in the unknown computers tab. You should use caution when you deploy client software to devices that appear in the unmanaged computers tab. Verify that these devices are valid targets for client software deployment.

You can also deploy client software by using the Push Deployment Wizard.

To deploy client software by using Find Unmanaged Computers

1 In the Symantec Endpoint Protection Manager console, click **Clients**.

2 In the Tasks pane, click **Find Unmanaged Computers**.

3 In the Find Unmanaged Computers window, under Search By, check **IP address range**, and enter the IP addresses for the range to search.

   Scanning a range of 100 IP addresses that do not exist takes approximately 5.5 minutes. Optionally, specify a computer name.

4. Under Logon Credentials, complete the User name, Password, and Domain-Workgroup boxes with the logon credentials that permit administration and installation.
5. Click **Search Now**.
6. On either the Unknown Computers or Unmanaged Computers tabs, do one of the following:
   - Check each computer on which you want to install client software.
   - Click **Select All**.
7. Under Installation, select the installation package, the installation option, and the features that you want to install.
8. To install to a group other than the default group, click **Change**, select a different group, and then click **OK**.
9. When you are ready to install the client software, click **Start Installation**.

About adding client installation package updates and upgrading clients

When Symantec provides updates to client installation packages, you first add them to a Symantec Endpoint Protection Manager and make them available for exporting. You do not, however, have to reinstall them with client-deployment tools. The easiest way to update clients in groups with the latest software is to use the console to update the group that contains the clients. You should first update a group with a small number of test computers. You can also update clients with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings Policy permits updates.

See "Managing content for clients" on page 132.

Adding client installation package updates

You receive client installation package updates from Symantec, and then you add them to the site database to make them available for distribution from Symantec Endpoint Protection Manager. You can optionally export the packages during this procedure to make the package available for deployment to computers that do not contain client software.

See "About adding client installation package updates and upgrading clients" on page 126.

Note: An installation package that you import consists of two files. One file is named *product_name*.dat, and the other file is named *product_name*.info.

To add a client installation package update

1. Copy the package to a directory on the computer that runs the Symantec Endpoint Protection Manager.
2. In the console, click **Admin**, and then click **Install Packages**.
3. Under **Tasks**, click **Add Client Install Package**.
4. In the **Add Client Install Package** dialog box, type a name and a description for the package.
5. Click **Browse**.
6. In the **Select Folder** dialog box, locate and select the *product_name*.info file for the new package, and then click **Select**.
7. When the Completed successfully prompt appears, do one of the following:
   - If you do not want to export the installation files and make them available for deployment, click **Close**.
     You are finished with this procedure.
   - If you do want to export the installation files and make them available for deployment, click **Export this Package**, and then complete this procedure.
8. In the **Export Package** dialog box, click **Browse**.
9. In the **Select Export Folder** dialog box, browse to and select the directory to contain the exported package, and then click **OK**.
10. In the **Export Package** dialog box, select a group, and then set the other options according to your installation goals.
11. For details about setting other options in this dialog box, click **Help**.
12. Click **OK**.

Upgrading clients in one or more groups

You can update clients in one or more groups from the Admin pane and Client pane.

See "About adding client installation package updates and upgrading clients" on page 126.

Note: You have much greater control over the way the package is distributed if you update the clients from the Clients pane.

To update clients in one or more groups from the Admin page

1. In the console, click **Admin**, and then click **Install Packages**.
2. Under Tasks, click **Upgrade Groups with Package**.
3. In the Upgrade Groups Wizard panel, click **Next**.
4. In the Select Client Install Package panel, under Select the new client installation package, select the package that you added, and then click **Next**.
5. In the Specify Groups panel, check the groups that you want to upgrade, and then click **Next**.
6. In the Package Upgrade Settings panel, check **Download from the management server**, and then click **Next**.
7. In the Upgrade Groups Wizard Complete panel, click **Finish**.

To update clients in one or more groups from the Clients page

1. In the console, click **Clients**.
2. In the View Clients pane, select a group to which you assigned the package.
3. On the Install Packages tab, under Tasks, click **Add Client Install Package**.
4. On both the General and Notification tabs, select the options that control how you want to distribute the update.

   For details about setting other options, click **Help**.
5. When you finish configuring the update distribution options, click **OK**.

Deleting upgrade packages

Upgrade packages are stored in the database. Each of these upgrade packages requires up to 180 MB of database space, so you should delete the older software upgrade packages that you no longer need. You do not delete packages from the file system; they are only deleted from the database. Therefore, you can add them again if you need them at some future date.

See "About adding client installation package updates and upgrading clients" on page 126.

To delete upgrade packages

1. In the console, click **Admin**.
2. Under Tasks, click **Install Packages**.
3. In the Client Install Packages pane, select the package to delete.
4. Under Tasks, click **Delete Client Install Package**.
5. In the Delete Client Install Package dialog box, click **Yes**.

Chapter 8

Updating definitions and content

This chapter includes the following topics:

- Enabling third-party content distribution to managed clients with a LiveUpdate Settings Policy
- Distributing content to managed clients with third-party distribution tools
- About using third-party distribution tools to distribute content updates to self-managed clients
- Running LiveUpdate on a client from the console

Managing content for clients

Clients periodically receive updates to virus and spyware definitions, IPS signatures, and product software. LiveUpdate is the name of the technology that distributes these content updates to clients or to servers that distribute the content to clients.

Table 8-1 Content update management

Task	Description
Decide on a distribution method	By default, clients get updates from the default management server (Symantec Endpoint Protection Manager). **Note:** Mac clients get updates only from an internal or an external LiveUpdate server. Typically, your network architecture determines which distribution method you should use. You use a LiveUpdate Settings Policy to configure the distribution method. You can also configure the schedule for clients to receive content from directly Symantec LiveUpdate. See "Determining how clients get content" on page 134. See "Configuring a LiveUpdate Settings policy " on page 143.
Decide what content clients should download	By default, the client computers receive updates for all of the content types. You can configure a LiveUpdate Content Policy to control the types of content updates to your clients. This policy type is not supported for Symantec Network Access Control clients. **Note:** If you use the default management server to distribute content updates to clients, the management server must also be configured to download the same updates. Otherwise, those updates are not available for group distribution. See "About the types of content" on page 133.

Table 8-1 Content update management *(continued)*

Task	Description
Configure a site to download content updates	The site that includes the default management server must store the content updates that you want to distribute to clients. You can also configure how often the site receives LiveUpdate content. See "Configuring a site to download content updates" on page 139. **Note:** If replication is used, only one site needs to be configured to download update files. Replication automatically updates the other database. As a best practice, however, you should not replicate product updates between sites. These updates can be quite large and one exists for every language that you select. If you select to download product updates with LiveUpdate to Symantec Endpoint Protection Manager, the updates automatically appear in the **Installation Packages** pane. You can then update clients with auto-upgrade. If you use this approach for version control, you should not select automatic product upgrades in the LiveUpdate Settings Policy. If you do not want to use LiveUpdate, you can use the Intelligent Updater to download content manually to the default management server. You can then distribute content with third-party management tools. See "Using the Intelligent Updater to download antivirus content updates for distribution" on page 155. See "Distributing content to managed clients with third-party distribution tools" on page 159.

About the types of content

Content includes virus and spyware definitions, IPS signatures, and product software. You use the properties settings for the site to control the content downloads to the default management server. You use a LiveUpdate Content Policy to control the content types that you want to download to your clients.

See "Managing content for clients" on page 132.

Note: LiveUpdate content includes definitions and content. It does not include policy updates. Symantec Endpoint Protection Manager updates policies on clients when you assign a new policy to a group or when you edit an existing policy.

Table 8-2 lists the types of content.

Table 8-2 Content types

Content type	Description
Client updates	Includes the product updates to client software.
Virus and spyware definitions	Contains two types of updates, full-version update and direct-delta update. The type of the update is included in the update package. Separate virus definition packages are available for the x86 and the x64 platforms.
Decomposer signatures	Supports the Antivirus and Antispyware Protection engine, and are used to decompose and read the data that is stored in various formats.
TruScan proactive threat scan heuristic signatures	Protects against zero-day attack threats.
TruScan proactive threat scan commercial application list	Includes the legitimate commercial applications that have generated false positives in the past.
Intrusion Prevention signatures	Protects against network threats and support the intrusion prevention and detection engines.
Submission Control signatures	Controls the flow of submissions to Symantec Security Response.
Host Integrity templates	Includes the predefined requirements that enforce updated patches and security measures on the client computer. Only available in the **Site Properties** dialog box when you install Symantec Network Access Control.

Determining how clients get content

Several content distribution methods are available to update clients. The content distribution methods that you use depend on the following factors:

- How you set up your network
- How many clients you manage
- Whether you manage Windows and Mac clients

Warning: Mac clients get updates only from an internal or an external LiveUpdate server.

Only Windows clients can get updates from the default management server or from a Group Update Provider.

Table 8-3 Content distribution methods and when to use them

Method	Description	When to use it
Symantec Endpoint Protection Manager to clients (Default)	The default management server can update the clients that it manages. You might have multiple management servers in your Symantec Endpoint Protection Manager network. The site that includes the management servers receives LiveUpdate content.	This method is configured by default after management server installation. You can also combine this method with a Group Update Provider. See "Configuring a LiveUpdate Settings policy " on page 143.
Group Update Provider to clients	A Group Update Provider is a client that acts as a proxy between a Symantec Endpoint Protection Manager and the clients in the group. The Group Update Provider receives updates from a management server, and then forwards the updates to the other clients in the group. A Group Update Provider can update multiple groups.	Use this method for groups co-located at remote locations with minimal bandwidth. Also, this method reduces the load on the management servers. Note that a Group Update Provider distributes all types of LiveUpdate content except client software updates. See "Distributing content using Group Update Providers" on page 147.

Table 8-3 Content distribution methods and when to use them *(continued)*

Method	Description	When to use it
Internal LiveUpdate server to clients	Clients can pull updates directly from an internal LiveUpdate server that receives updates from Symantec LiveUpdate. You can set up an internal LiveUpdate server on a computer whether Symantec Endpoint Protection Manager software is installed or not. In either case, you should use the LiveUpdate Administrator utility to update the LiveUpdate server. The LiveUpdate Administrator utility pulls the definitions updates down from a Symantec LiveUpdate server. The utility then places the packages on a Web server, an FTP site, or a location that is designated with a UNC path. You must then configure your management servers to pull their definitions updates from this location.	Use an internal LiveUpdate server in large networks to reduce the load on the Symantec Endpoint Protection Manager. You typically use an internal LiveUpdate server in large networks of more than 10,000 clients. With this architecture, the management server offloads the LiveUpdate content update functionality, but still processes logs and policy updates. The internal LiveUpdate server is also useful for the networks that run multiple Symantec products that also run LiveUpdate to update clients. For more information about setting up an internal LiveUpdate server, see the *LiveUpdate Administrator User's Guide*. The guide is available on the installation CD and on the Symantec Support Web site. See "Configuring a LiveUpdate Settings policy " on page 143.
Symantec LiveUpdate to clients	Clients can receive updates directly from Symantec LiveUpdate.	Use an external Symantec LiveUpdate server for the self-managed client computers that are not always connected to the corporate network. **Note:** Do not configure large numbers of managed, networked clients to pull updates from an external Symantec LiveUpdate server. This configuration consumes unnecessary amounts of Internet bandwidth. See "Configuring a LiveUpdate Settings policy " on page 143.

Table 8-3 Content distribution methods and when to use them *(continued)*

Method	Description	When to use it
Third-party tool distribution (Not illustrated)	Third-party tools like Microsoft SMS let you distribute specific update files to clients.	Use this method when you want to test update files before distributing them. Also, use this method if you have a third-party tool distribution infrastructure, and want to leverage the infrastructure. See "Distributing content to managed clients with third-party distribution tools" on page 159.
Intelligent Updater	Intelligent Updater downloads content manually. You can retrieve Intelligent Updater self-extracting files from the Symantec Web site that contain virus and security risk definitions files with jdb and vdb extensions. Idb extensions are no longer supported. To receive other update files, you must set up and configure a management server to download and stage the update files.	You can use Intelligent Updater if you do not want to use Symantec LiveUpdate or LiveUpdate is not available. See "Using the Intelligent Updater to download antivirus content updates for distribution" on page 155.

Figure 8-1 shows an example distribution architecture for smaller networks.

Figure 8-1 Example distribution architecture for smaller networks

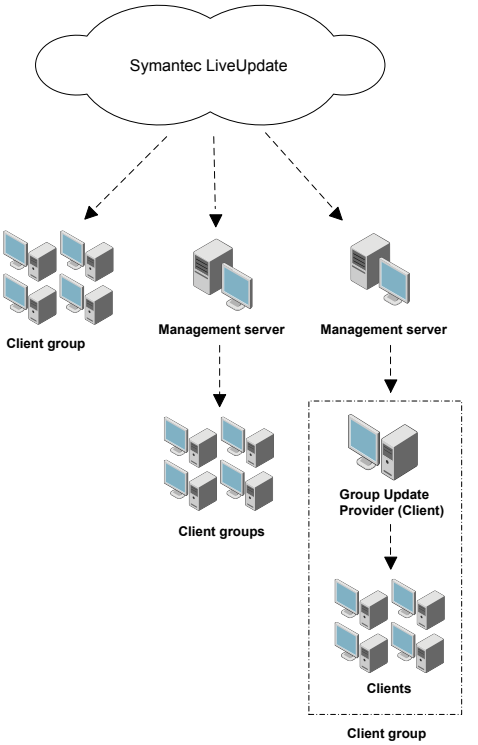
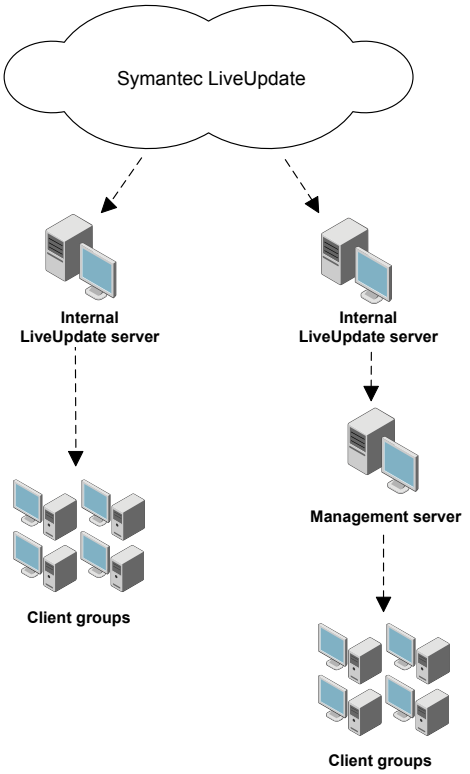


Figure 8-2 shows an example distribution architecture for larger networks.

Figure 8-2 Example distribution architecture for larger networks



Configuring a site to download content updates

When you configure a site to download LiveUpdate content, you make the following decisions:

- How often the site checks for LiveUpdate content updates.
  The default schedule of having Symantec Endpoint Protection Manager run LiveUpdate every 4 hours is a best practice.

  Note: Sites download MSP files for product updates, and then create new MSI files. Sites replicate MSI files if you select to replicate product updates. The MSP files are a fraction of the size of the MSI files.

- What content types to download to the site.

Make sure that the site downloads all content updates that are specified in your client LiveUpdate Content Policies.

- The languages for update types to download.
- The LiveUpdate server that serves the content to the site.
  You can specify either an external Symantec LiveUpdate server (recommended), or an internal LiveUpdate server that has previously been installed and configured.
- The number of content revisions to keep and whether to store the client packages unzipped.
  You store content revisions because you might want to test the latest content before you roll it out to all your clients. You might want to keep earlier versions of the content so that you can roll back if necessary.

Note: When you keep a large number of revisions, more disk space is required on the Symantec Endpoint Protection Manager.

See "Managing content for clients" on page 132.

To configure a site to download updates

1. In the console, click **Admin**.
2. Under **Tasks**, click **Servers**.
3. In the **View** pane, right-click **Local Site**, and then click **Edit Properties**.
4. In the **Site Properties** dialog box, on the **LiveUpdate** tab, under **Download Schedule**, set the scheduling options for how often the server should check for updates.
5. Under **Content Types to Download**, inspect the list of update types that are downloaded.
6. To add or delete an update type, click **Change Selection**, modify the list, and then click **OK**.

   The list should match the list of content types that you include in the LiveUpdate Content Policy for your client computers.
7. Under **Languages to Download**, inspect the list of languages of the update types that are downloaded.
8. To add or delete a language, click **Change Selection**, modify the list, and then click **OK**.

9 Under **LiveUpdate Source Servers**, inspect the current LiveUpdate server that is used to update the management server. This server is Symantec LiveUpdate server by default. Then do one of the following:

- To use the existing LiveUpdate Source server, click **OK**.
- To use an internal LiveUpdate server, click **Edit Source Servers**.

10 If you selected **Edit Source Servers**, in the **LiveUpdate Servers** dialog box, click **Use a specified internal LiveUpdate server**, and then click **Add**.

11 In the **Add LiveUpdate Server** dialog box, complete the boxes with the information that identifies the LiveUpdate server, and then click **OK**.

For failover support, you can install, configure, and select more than one LiveUpdate server. If one server goes offline, the other server provides support.

12 In the **LiveUpdate Servers** dialog box, click **OK**.

13 Under **Disk Space Management for Downloads**, type the number of LiveUpdate content revisions to keep.

More disk space is required for the storage of a large number of content revisions. Client packages that are stored in expanded format also require more disk space.

14 Check or uncheck **Store client packages unzipped to provide better network performance for upgrades**.

15 Click **OK**.

About simultaneous content downloads

The Symantec Endpoint Protection Manager supports randomization of simultaneous content downloads to your clients from the default management server or a Group Update Provider. It also supports the randomization of the content downloads from a LiveUpdate server to your clients. Randomization reduces peak network traffic and is on by default.

You can enable or disable the randomization function. The default setting is enabled. You can also configure a randomization window. The management server uses the randomization window to stagger the timing of the content downloads. Typically, you should not need to change the default randomization settings.

In some cases, however, you might want to increase the randomization window value. For example, you might run the Symantec Endpoint Protection client on multiple virtual machines on the same physical computer that runs the

management server. The higher randomization value improves the performance of the server but delays content updates to the virtual machines.

You also might want to increase the randomization window when you have many physical client computers that connect to a single server that runs the management server. In general, the higher the client-to-server ratio, the higher you might want to set the randomization window. The higher randomization value decreases the peak load on the server but delays content updates to the client computers.

In a scenario where you have very few clients and want rapid content delivery, you can set the randomization window to a lower value. The lower randomization value increases the peak load on the server but provides faster content delivery to the clients.

For downloads from the default management server or a Group Update Provider, you configure the randomization settings in the Communication Settings dialog box for the selected group. The settings are not part of the LiveUpdate Settings Policy.

For downloads from a LiveUpdate server to your clients, you configure the randomization setting as part of the LiveUpdate Settings Policy.

See "Configuring a LiveUpdate Settings policy " on page 143.

About LiveUpdate Policies

Two types of LiveUpdate Policies exist. One type is called a LiveUpdate Settings Policy and applies to Symantec Endpoint Protection and Symantec Network Access Control clients. The other type is called a LiveUpdate Content Policy and applies to Symantec Endpoint Protection clients only. The LiveUpdate Settings Policy specifies the computers that clients contact to check for updates, and controls how often clients check for updates. If required, you can apply this policy to specific locations in a group.

See "Configuring a LiveUpdate Settings policy " on page 143.

The LiveUpdate Content Policy specifies the update types that clients are permitted to check for and install. For each type, you can specify that clients check for and install the latest update. Or, you can specify a version of an update that clients install if they do not run that version. You cannot apply this policy to specific locations in a group. You can apply this policy only at the group level.

See "Configuring a LiveUpdate Content Policy" on page 145.

About using the content revisions that are not the latest version

If you store multiple versions of content in the Symantec Endpoint Protection Manager, you might want to specify a particular revision in your LiveUpdate Content Policy. For example, you can test the latest revision before you roll it out to clients. You can specify an older revision in the policy.

In some cases, the revision that is specified in the policy does not match the revisions that are stored on the Symantec Endpoint Protection Manager. For example, you might import a policy that references a revision that does not exist on the server. Or, you might replicate policies but not LiveUpdate content from another site. In both cases, the policy shows that the revision is not available. Even though the revision is not available on the server, the clients that use the policy are still protected. The clients use the latest revision of the content.

See "Configuring a LiveUpdate Content Policy" on page 145.

Configuring a LiveUpdate Settings policy

When you add and apply a LiveUpdate Settings policy , you should have a plan for how often you want client computers to check for updates. The default setting is every four hours. You should also know the place from which you want your client computers to check for and get updates. If possible, you want client computers to check for and get updates from the Symantec Endpoint Protection Manager. After you create your policy, you can assign the policy to one or more groups and locations.

Note: Mac clients must get updates from LiveUpdate or manually.

See "Using the Intelligent Updater to download antivirus content updates for distribution" on page 155.

Note: An advanced setting is available to let users manually start LiveUpdate from their client computers. This setting is disabled by default. If you enable this setting, users can start LiveUpdate and download the latest content virus definitions, component updates, and product updates. Depending on the size of your user population, you may not want to let users download all content without previous testing. Additionally, conflicts can occur if two LiveUpdate sessions run simultaneously on client computers. By default, users are not allowed to download product updates from a LiveUpdate server. You can change this setting in the **Advanced Settings** panel of the LiveUpdate policy.

Note: Users can always run LiveUpdate on Mac clients. You can restrict only Windows clients from running LiveUpdate. Product updates from a LiveUpdate server, however, can be restricted on both Mac and Windows clients. If you restrict product updates from LiveUpdate on a Mac client, you must provide them manually. Mac clients cannot get updates from the management server.

To configure a LiveUpdate Settings policy

1. In the console, click **Policies**.
2. Under **View Policies**, click **LiveUpdate**.
3. On the **LiveUpdate Settings** tab, under **Tasks**, click **Add a LiveUpdate Settings Policy**.
4. In the **Overview** pane, in the **Policy name** box, type a name for the policy.
5. Under **LiveUpdate Policy**, click **Server Settings**.
6. In the **Server Settings** pane, under **Internal or External LiveUpdate Server**, select at least one content distribution method.

   Most organizations should use the default management server. If you select the default management server in an environment that contains Mac and Windows computers, Mac clients get their updates from the default LiveUpdate server.

   See "Determining how clients get content" on page 134.
7. If you selected Use a LiveUpdate server, under **LiveUpdate Policy**, click **Schedule**.
8. In the **Schedule** pane, accept or change the scheduling options.
9. If you selected Use a LiveUpdate server, under **LiveUpdate Policy**, click **Advanced Settings**.
10. Decide whether to keep or change the default settings.

    Generally, you do not want users to modify update settings. You may, however, want to let them manually launch a LiveUpdate session if you do not support hundreds or thousands of clients.
11. When you have configured your policy, click **OK**.
12. In the **Assign Policy** dialog box, do one of the following:
    - Click **Yes** to save and assign the policy to a group or location in a group.

- Click **No** to save the policy only.

13 If you clicked Yes, in the **Assign LiveUpdate Policy** dialog box, check the groups and locations to which to assign the policy, and then click **Assign**.

If you cannot select a nested group, that group inherits policies from its parent group, as set on the **Policies** tab of the **Clients** page.

Configuring a LiveUpdate Content Policy

By default, all Symantec Endpoint Protection clients in a group receive the latest versions of all content and all product updates. If a client group gets updates from a management server, the clients receive only the updates that the server is configured to download. For example, you might configure the LiveUpdate Content Policy to permit all updates. If the management server is not configured to download all updates, the clients receive only what the server downloads.

See "Configuring a site to download content updates" on page 139.

If a group is configured to get updates from a LiveUpdate server, the group's clients receive all updates permitted in the LiveUpdate Content Policy. If the LiveUpdate Content Policy specifies a specific revision of content, the clients do not receive the latest available content.

You might want to specify that your clients receive a specific revision. With that configuration, you can test the latest version first before you distribute it to clients. While you test the latest version, your clients use the specified revision. After you test the version, you can modify the LiveUpdate Content Policy to specify that clients receive the latest version of the content.

Note: Using specific revisions provides rollback functionality.

To configure a LiveUpdate Content Policy

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

2 Under **View Policies**, click **LiveUpdate**.

3 Click the **LiveUpdate Content** tab.

4 Under **Tasks**, click **Add a LiveUpdate Content Policy**.

5 In the **Overview** pane, in the **Policy name** box, type a name for the policy.

6 In the **LiveUpdate Content** pane, click **Security Definitions**.

7 In the **Security definitions** pane, check the updates to download and install, and uncheck the updates to disallow.

Note: Mac clients can install only updates to antivirus and antispyware definitions.

8 For each update, do one of the following actions:

- Check **Use latest available**
- Check **Select a revision**

9 To continue, do one of the following:

- If you did not check **Select a revision** for an update type, click **OK**, and then continue with step 12.
- If you did check **Select a revision** for an update type, click **Edit**, and then continue with the next step.

10 In the **Select Revision** dialog box, in the Revision column, select the revision to use, and then click **OK**.

11 In the **LiveUpdate Content** window, click **OK**.

12 In the **Assign Policy** dialog box, click **Yes**.

You can optionally cancel out of this procedure, and assign the policy at a later time.

13 In the **Assign LiveUpdate Content Policy** dialog box, check one or more groups to which to assign this policy, and then click **Assign**.

Viewing and changing the LiveUpdate Content Policy quickly

LiveUpdate Content Policies are applied to groups and to all locations in groups. Unlike many other policy types, a LiveUpdate Content Policy is not location-specific.

See "Configuring a LiveUpdate Content Policy" on page 145.

You can view and change the LiveUpdate Policy quickly in the console from the Clients tab.

To view and change the LiveUpdate Content Policy that is applied to a group

1. In the console, click **Policies**, and create at least two LiveUpdate Content Policies.
2. Apply one of the policies to a group.
3. Click **Clients**.
4. On the **Policies** tab, under Settings in the right-hand pane, click **LiveUpdate Content Policy Settings**.
5. In the **LiveUpdate Content Policy** dialog box, note the name of the currently used policy under **Specify the LiveUpdate Content Policy to use for this group**.
6. To change the policy that is applied to the group, select the policy that you want to use, and then click **OK**.

Distributing content using Group Update Providers

A Group Update Provider is a client computer that you designate to locally distribute content updates to clients. A Group Update Provider downloads content updates from the management server and distributes the updates to clients.

A Group Update Provider helps you conserve bandwidth by offloading processing power from the server to the Group Update Provider.

A Group Update Provider is ideal for delivering content updates to clients that have limited network access to the server. You can use a Group Update Provider to conserve bandwidth to clients in a remote location over a slow link.

Table 8-4 Managing Group Update Providers

Step	Action	Description
Step 1	Verify client communication	Before you configure Group Update Providers, verify that the clients can receive content updates from the server. Resolve any client-server communication problems. You can view client-server activity in the System logs. See "Viewing logs" on page 267.

Table 8-4 Managing Group Update Providers *(continued)*

Step	Action	Description
Step 2	Configure Group Update Providers	You configure Group Update Providers by specifying settings in the LiveUpdate Settings Policy. You can configure a single Group Update Provider or multiple Group Update Providers. See "Configuring a Group Update Provider" on page 151.
Step 3	Assign the LiveUpdate Settings Policy to groups	You assign the LiveUpdate Settings Policy to the groups that use the Group Update Providers. You also assign the policy to the group in which the Group Update Provider resides. For a single Group Update Provider, you assign one LiveUpdate Settings Policy per group per site. For multiple Group Update Providers, you assign one LiveUpdate Settings Policy to multiple groups across subnets. See "Assigning a shared policy" on page 98. See "About the types of Group Update Providers" on page 148.
Step 4	Verify that clients are designated as Group Update Providers	You can view the client computers that are designated as Group Update Providers. You can search client computers to view a list of Group Update Providers. A client computer's properties also shows whether or not it is a Group Update Provider. See "Searching for the clients that act as Group Update Providers" on page 154. See "Viewing a client's properties" on page 72.

About the types of Group Update Providers

You can configure two types of Group Update Providers: a single Group Update Provider or multiple Group Update Providers:

- Single Group Update Provider

  A single Group Update Provider is a dedicated client computer that provides content for one or more groups of clients. A single Group Update Provider can be a client computer in any group. To configure a single Group Update Provider,

you specify the IP address or host name of the client computer that you want to designate as the Group Update Provider.

- Multiple Group Update Provider
  Multiple Group Update Providers use a set of rules, or criteria, to elect themselves to serve groups of clients across subnets. To configure multiple Group Update Providers, you specify the criteria that client computers must meet to qualify as a Group Update Provider. If a client computer meets the criteria, the Symantec Endpoint Protection Manager adds the client to its list of Group Update Providers. Symantec Endpoint Protection Manager then makes the list available to all the clients in your network. Clients check the list and choose the Group Update Provider that is located in their subnet. You can also configure a single, dedicated Group Update Provider to distribute content to clients when the local Group Update Provider is not available.

You use a LiveUpdate Settings Policy to configure the type of Group Update Provider. The type you configure depends on how your network is set up and whether or not your network includes legacy clients.

Table 8-5 When to use a particular Group Update Provider type

Group Update Provider Type	When to use
Single	Use a single Group Update Provider when your network includes any of the following scenarios: ■ Your network includes legacy clients Legacy clients can get content from a single Group Update Provider; legacy clients can also be designated as a Group Update Provider. Legacy clients do not support multiple Group Update Providers. ■ You want to use the same Group Update Provider for all your client computers You can use a single LiveUpdate Content Settings Policy to specify a static IP address or host name for a single Group Update Provider. However, if clients change locations, you must change the IP address in the policy. If you want to use different Group Update Providers in different groups, you must create a separate LiveUpdate Settings Policy for each group. See "Configuring a single Group Update Provider" on page 152.

Table 8-5 When to use a particular Group Update Provider type *(continued)*

Group Update Provider Type	When to use
Multiple	Use multiple Group Update Providers when your network includes any of the following scenarios: ■ You run the latest client software on the computers in your network Multiple Group Update Providers are supported on the computers that run the latest client software. Multiple Group Update Providers are not supported by legacy clients. Legacy clients cannot get content from multiple Group Update Providers. Legacy clients cannot be designated as a Group Update Provider even if they meet the criteria for multiple Group Update Providers. You can create a separate LiveUpdate Settings Policy and configure a single, static Group Update Provider for a group of legacy clients ■ You have multiple groups and want to use different Group Update Providers for each group You can use one policy that specifies rules for the election of multiple Group Update Providers. If clients change locations, you do not have to update the LiveUpdate Settings Policy. The Symantec Endpoint Protection Manager combines multiple Group Update Providers across sites and domains. It makes the list available to all clients in all groups in your network. ■ Multiple Group Update Providers can function as a failover mechanism. Multiple Group Update Providers ensure a higher probability that at least one Group Update Provider is available in each subnet. See "Configuring multiple Group Update Providers" on page 153.

About configuring rules for multiple Group Update Providers

Multiple Group Update Providers use rules to determine which client computers act as a Group Update Provider.

Rules are structured as follows:

- Rule sets
  A rule set includes the rules that a client must match to act as a Group Update Provider.
- Rules
  Rules can specify IP addresses, host names, Windows client registry keys, or client operating systems. You can include one of each rule type in a rule set.
- Rule conditions

A rule specifies a condition that a client must match to act as a Group Update Provider. If a rule specifies a condition with multiple values, the client must match one of the values.

Table 8-6 Rule types

Rule type	Description
IP address or host name	This rule specifies client IP addresses or host names.
Registry keys	This rule specifies Windows client registry keys.
Operating system	This rule specifies client operating systems.

Rules are matched based on the logical OR and AND operators as follows:

- Multiple rule sets are OR'ed. A client must match one rule set.
- Multiple rules are AND'ed. A client must match all the rules that are specified in a rule set.
- Multiple values for a rule condition are OR'ed. A client must match one value.

For example, you might create RuleSet 1 that includes an IP address rule with several IP addresses. You then create RuleSet2 that includes a host name rule and an operating system rule each with multiple values. A client computer must match either RuleSet1 or RuleSet2. A client matches RuleSet1 if it matches any one of the IP addresses. A client matches RuleSet2 if it matches any one of the host names and any of the operating systems.

See "Configuring multiple Group Update Providers" on page 153.

Configuring a Group Update Provider

You configure a Group Update Provider by specifying settings in the LiveUpdate Settings Policy.

You can configure the LiveUpdate Settings Policy so that clients only get updates from the Group Update Provider and never from the server. You can specify when clients must bypass the Group Update Provider. You can configure settings for downloading and storing content updates on the Group Update Provider computer. You can also configure the type of Group Update Provider.

Note: If the Group Update Provider runs a non-Symantec firewall, you might need to modify the firewall to permit the TCP port to receive server communications. By default, the Symantec Firewall Policy is configured correctly.

To configure a Group Update Provider

1. In the console, click **Policies**.
2. Under **View Policies**, click **LiveUpdate**.
3. In the **LiveUpdate Policies** pane, on the **LiveUpdate Settings** tab, select the policy to edit.
4. In the **Tasks** pane, click **Edit the Policy**.
5. In the **LiveUpdate Policy** window, click **Server Settings**.
6. On the **Server Settings** page, under **Internal or External LiveUpdate Server**, check **Use the default management server (Windows computers only)**.

   Do not check **Use a LiveUpdate server**. The Group Update Provider that you configure acts as the default LiveUpdate server.
7. Under **Group Update Provider**, check **Use a Group Update Provider**.
8. Click **Group Update Provider**.
9. In the **Group Update Provider** dialog box, configure the type of Group Update Provider.

   Note: Legacy clients can only use a single Group Update Provider. Legacy clients do not support multiple Group Update Providers.

   See "Configuring a single Group Update Provider" on page 152.

   See "Configuring multiple Group Update Providers" on page 153.
10. In the **Group Update Provider** dialog box, configure the options to control how content is downloaded and stored on the Group Update Provider computer.

    Click **Help** for information about content downloads.
11. Click **OK**.

    See "Distributing content using Group Update Providers" on page 147.

Configuring a single Group Update Provider

You can configure only one single Group Update Provider per LiveUpdate Settings Policy per group. To create a single Group Update Provider for multiple sites, you must create one group per site, and one LiveUpdate Settings Policy per site.

To configure a single Group Update Provider

1. Follow the steps to configure a Group Update Provider.

   See "Configuring a Group Update Provider" on page 151.

2. In the **Group Update Provider** dialog box, under **Group Update Provider Selection for Client**, check **Single Group Update Provider IP address or host name**.

3. In the **Single Group Update Provider IP address or host name** box, type the IP address or host name of the client computer that acts as the single Group Update Provider.

   Click **Help** for information about the IP address or host name.

   See "About the types of Group Update Providers" on page 148.

   See "Configuring multiple Group Update Providers" on page 153.

   See "Distributing content using Group Update Providers" on page 147.

Configuring multiple Group Update Providers

You can configure multiple Group Update Providers by specifying criteria in a LiveUpdate Settings Policy. Clients use the criteria to determine if they qualify to act as a Group Update Provider.

To configure multiple Group Update Providers

1. Follow the steps to configure a Group Update Provider.

   See "Configuring a Group Update Provider" on page 151.

2. In the **Group Update Provider** dialog box, under **Group Update Provider Selection for Client**, check **Multiple Group Update Providers**.

3. Click **Configure Group Update Provider List**.

4. In the **Group Update Provider List** dialog box, select the tree node **Group Update Provider**.

5. Click **Add** to add a rule set.

6. In the **Specify Group Update Provider Rule Criteria** dialog box, in the **Check** drop-down list, select one of the following:

   - **Computer IP Address or Host Name**
   - **Registry Keys**
   - **Operating System**

7. If you selected Computer IP Address/Host Name or Registry Keys, Click **Add**.

8 Type or select the IP address or host name, Windows registry key, or operating system information.

Click **Help** for information on configuring rules.

See "About configuring rules for multiple Group Update Providers" on page 150.

9 Click **OK** until you return to the **Group Update Provider** dialog box.

10 In the **Group Update Provider List** dialog box, optionally add more rule sets.

11 Type a Group Update Provider IP address or host name in the **Specify the host name or IP address of a Group Update Provider on a different subnet to be used, if Group Update Providers on the local subnet are unavailable** text box.

12 Click **OK**.

See "Distributing content using Group Update Providers" on page 147.

Searching for the clients that act as Group Update Providers

You can verify that clients are available as Group Update Providers. You can view a list of Group Update Providers by searching for them on the **Clients** tab.

Note: You can also check a client's properties. The properties include a field that indicates whether or not the client is a Group Update Provider.

To search for the clients that act as Group Update Providers

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

2 On the **Clients** page, on the **Clients** tab, in the **View** box, select **Client status**.

3 In the **Tasks** pane, click **Search Clients**.

4 In the **Find** box, select **Computers**.

5 In the **In Group** box, specify the group name.

6 Under **Search Criteria**, in the **Search Field** column, select **Group Update Provider**.

7 Under **Search Criteria**, in the **Comparison Operator** column, select **=**.

8 Under **Search Criteria**, in the **Value** column, select **True**.

Click **Help** for information on the search criteria.

9 Click **Search**.

See "Distributing content using Group Update Providers" on page 147.

About the Intelligent Updater

You can use the Intelligent Updater to download virus and security risk content updates to your management server. Symantec recommends that you use LiveUpdate to update content. However, in situations where you do not want to use LiveUpdate or LiveUpdate is not available, you can use the Intelligent Updater. After you download the files, you can use your preferred distribution method to update your clients.

Note: The Intelligent Updater only provides virus and security risk content updates. It does not provide updates for any other type of content.

The Intelligent Updater is available as a single file or as a split package, which is distributed across several smaller files. The single file is for computers with network connections. The split package is for the computers that do not have network connections, Internet access, or a CD-ROM drive. Copy the split package to removable media for distribution.

See "Using the Intelligent Updater to download antivirus content updates for distribution" on page 155.

Note: Antivirus and antispyware definitions are contained in the vdb and jdb files that you can distribute. Vdb files support 32-bit clients only. Jdb files support both 32-bit clients and 64-bit clients. These are the files that you place in client computer's inboxes. You can download updates from the following site:

ftp://ftp.symantec.com/AVDEFS/symantec_antivirus_corp/

Using the Intelligent Updater to download antivirus content updates for distribution

To distribute updated virus and security risk updates only, download a new Intelligent Updater. Then, use your preferred distribution method to deliver the updates to your clients.

Note: Currently, Intelligent Updater updates virus and security risk updates only. Make sure to use Intelligent Updater files for the enterprise version rather than the consumer version of the product.

See "About the Intelligent Updater" on page 155.

To download Intelligent Updater

1. Using your Web browser, go to the following URL:

   http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=savce

2. Click the appropriate product file with the .exe extension.
3. When you are prompted for a location in which to save the files, select a folder on your hard drive.

To install the virus and security risk definitions files

1. Locate the Intelligent Updater file that you downloaded from Symantec.
2. Double-click the file and follow the on-screen instructions.

About the files that are used in third-party distribution of LiveUpdate content

The Symantec Endpoint Protection third-party distribution procedure uses a file called index2.dax. The LiveUpdate-related content of the index2.dax file includes a set of content monikers and their associated sequence numbers. Each content moniker corresponds to a particular content type. Each sequence number in the index2.dax file corresponds to a revision of a particular content type.

You can see a mapping of the moniker to its content type by opening the ContentInfo.txt file. The file is typically located in the \Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\content folder.

For example, you might see the following entry:

```
{C60DC234-65F9-4674-94AE-62158EFCA433}: SESC Virus Definitions
Win32 v11 - MicroDefsB.CurDefs - SymAllLanguages
```

There is an index2.dax file for each client group. The file is located in the folder that corresponds to the group policy serial number. The serial number is listed in the Group Properties dialog box. The first four hexadecimal values in the serial number should match the first four hexadecimal values of one of the folder names.

The index2.dax file is encrypted. To look at the contents of the file, you can open index2.xml, which is available in the same folder. You can see a listing of the content monikers with their sequence (revision) numbers. For example, you might see the following entry:

```
<File Checksum="191DEE487AA01C3EDA491418B53C0ECC" DeltaFlag="1"
FullSize="30266080" LastModifiedTime="1186471722609" Moniker=
"{C60DC234-65F9- 4674-94AE-62158EFCA433}" Seq="80806003"/>
```

The LiveUpdate Content Policy on the clients to which you are distributing content specifies a particular revision of content or the latest content. The sequence number in the index2.dax file that you use for the distribution must match the sequence number that corresponds to the content specified in the LiveUpdate Content Policy for the group. For example, if the LiveUpdate Content policy is set to "Use latest available" for all content types, then the sequence number for each content type is set to the latest content that is available on the Symantec Endpoint Protection Manager. In this example, the distribution only works if the index2.dax file that you use for distribution calls out the sequence numbers (revisions) that correspond to the latest content revision. The distribution fails if the sequence numbers correspond to any other revisions.

See "Distributing content to managed clients with third-party distribution tools" on page 159.

About using third-party distribution tools to distribute content updates to managed clients

Large networks might rely on third-party distribution tools like IBM Tivoli, Microsoft SMS, and so on to distribute updates to client computers. Symantec client software supports update distribution with these tools. To use third-party distribution tools, you need to get the update files, and you need to distribute the update files with a distribution tool.

For managed clients, you can get the update files after installing and configuring a Symantec Endpoint Protection Management server as the only server at a site. You then schedule and select the LiveUpdate content updates to download to the site.

See "Configuring a site to download content updates" on page 139.

The update files are downloaded into sub-directories in the following (default) directory:

\Program Files\Symantec Endpoint Protection Manager\data\outbox\

You then distribute the files to the inbox folder on client computers.

By default, this folder does not exist, and client software does not check and process content in this folder. For managed clients, you must configure a LiveUpdate Settings Policy for the group, enable third-party distribution to clients in the group, and assign the policy. The inbox folder then appears on the client computers in the group. For unmanaged clients, you must manually enable a Windows registry key on the client computers.

The inbox folder appears in the following location on the client computers that do not run Windows Vista:

\\Documents and Settings\All Users\Application Data\Symantec\ Symantec Endpoint Protection\inbox\

The inbox folder appears in the following location on the client computers that run Windows Vista:

\\Program Data\Symantec\Symantec Endpoint Protection\inbox\

See "Distributing content to managed clients with third-party distribution tools" on page 159.

Enabling third-party content distribution to managed clients with a LiveUpdate Settings Policy

When you create a LiveUpdate Policy that supports third-party content distribution to managed clients, you have a couple of additional goals. One goal is to reduce the frequency with which clients check for updates. The other goal typically is to disable the ability of client users to manually perform LiveUpdate. Managed clients are managed with Symantec Endpoint Protection Manager policies.

When you are finished with this procedure, the following directory appears on the group's client computers that do not run Windows Vista:

\\Documents and Settings\All Users\Application Data\Symantec\ Symantec Endpoint Protection\inbox\

The following directory appears on the group's client computers that do run Windows Vista:

\\Program Data\Symantec\Symantec Endpoint Protection\inbox\

To enable third-party content distribution to managed clients with a LiveUpdate Policy

1. In the console, click **Policies**.
2. Under **View Policies**, click **LiveUpdate**.
3. In the **LiveUpdate Policies** pane, on the **LiveUpdate Settings** tab, under **Tasks**, click **Add a LiveUpdate Setting Policy**.
4. In the **LiveUpdate Policy** window, in the **Policy name** and **Description** text boxes, type a name and description.
5. Click **Server Settings**.
6. Under **Third Party Management**, check **Enable third party content management**.

7 Uncheck all other LiveUpdate source options.

8 Click **OK**.

9 In the **Assign Policy** dialog box, click **Yes**.

You can optionally cancel out of this procedure, and assign the policy at a later time.

10 In the **Assign LiveUpdate Policy** dialog box, check one or more groups to which to assign this policy, and then click **Assign**.

Distributing content to managed clients with third-party distribution tools

After you configure the LiveUpdate Policy to enable third-party content management, you locate and copy the content on Symantec Endpoint Protection Manager. After you locate and copy the content, you distribute it to clients. You also decide what content to copy and distribute.

See "About using third-party distribution tools to distribute content updates to managed clients" on page 157.

See "About using third-party distribution tools to distribute content updates to self-managed clients" on page 160.

Note: If you stage update files on client computers before placing them in the /inbox directory, you must copy the files. Moving the files does not work. You can also copy .vdb and .jdb files to the inbox for processing.

To distribute content to managed clients with third-party distribution tools

1 On the computer that runs the Symantec Endpoint Protection Manager, create a working directory such as \Work_Dir.

2 In the console, on the Clients tab, right-click the group to update, and then click **Properties**.

3 Document the first four hexadecimal values of the Policy Serial Number, such as 7B86.

4 Navigate to the following directory:

\\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent

5 Locate the directory that contains the first four hexadecimal values that match your client group Policy Serial Number.

6 Open that directory, and then copy `index2.dax` to your working directory, such as \Work_Dir\index2.dax.

7 Navigate to the following directory:

\\Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\content

8 Open and read `ContentInfo.txt` to discover the content that each <<target moniker>> directory contains.

The contents of each directory is <<target moniker>>\<sequence num>\full.zip|full.

9 Copy the content of each \<<target moniker>> directory to your working directory such as \Work_Dir.

10 Delete all files and directories from each \<<target moniker>> so that only the following directory structure and file remain in your working directory:

\\Work_Dir\<<target moniker>>\<latest sequence number>\full.zip

Your working directory now contains the directory structure and files to distribute to your clients.

11 Use your third-party distribution tools to distribute the content of \Work_Dir to the \\Symantec Endpoint Protection\inbox\ directory on your clients in your group.

The end result must look like the following:

\\Symantec Endpoint Protection\inbox\index2.dax

\\Symantec Endpoint Protection\inbox\<<target moniker>>\<latest sequence number>\full.zip

If the files disappear so that \inbox\ is empty, you were successful. If an \inbox\invalid\ directory appears, you were not successful and must try again.

About using third-party distribution tools to distribute content updates to self-managed clients

If you installed self-managed clients from the installation CD, the clients do not trust and do not process LiveUpdate content or policy updates for security purposes. To enable these clients to process updates, you have to create the following Windows registry key: HKLM\Software\Symantec\Symantec Endpoint Protection\SMC\TPMState

Set the value to hexadecimal 80 so that the key looks like 0x00000080 (128)

After you set this key, you must either restart the computer or execute the following commands from the \Symantec\Symantec Endpoint Protection\ directory:

```
smc.exe -stop
```

```
smc.exe -start
```

The inbox folder appears in the following location on the client computers that do not run Windows Vista:

\\Documents and Settings\All Users\Application Data\Symantec\ Symantec Endpoint Protection\inbox\

The inbox folder appears in the following location on the client computers that do run Windows Vista:

\\Program Data\Symantec\Symantec Endpoint Protection\inbox\

You can now use third-party distribution tools to copy content or policy updates to this directory. The Symantec client software then trusts and process the content.

You get the content to distribute from a Symantec Endpoint Protection Manager almost the same way that you do for managed clients.

However, copy index2.xml from the My Company group, instead of copying index2.dax from your managed client group directory. Copy the full.dax file as described for the managed client. You can then distribute these files. You can also drop .vdb and .jdb files in the client inbox for processing.

Note: If you stage the update files on the computers, you must copy them to the inbox. The update files are not processed if you move them to the inbox.

Note: After a managed client installation, the TPMState Windows registry key exists with a value of 0, which you can change. (This key does not exist after an self-managed client installation.) Also, restarting the computer or smc.exe command execution is not required for a managed client installation. The directory appears as soon as the Windows registry key is changed.

See "Distributing content to managed clients with third-party distribution tools" on page 159.

See "About using third-party distribution tools to distribute content updates to managed clients" on page 157.

Running LiveUpdate on a client from the console

You can update content on clients by initiating LiveUpdate from the console. You can run a command on a single client or on a group of clients. The clients receive the latest content from Symantec LiveUpdate. Alternatively, you can initiate a LiveUpdate session and run an on-demand scan.

See "Running commands on clients from the console" on page 76.

To run LiveUpdate on a client from the console

1. In the console, click **Clients**, and then under **View Clients**, select a group.
2. On the **Clients** tab, do one of the following actions:
   - For all computers and users in a group, right-click the group, click **Run Command on Group**.
   - For selected computers or users within a group, select the group, right-click the computers or users, click **Run Command on Clients**.
3. Do one of the following actions:
   - Select **Update Content**.
   - Select **Update Content and Scan**.
4. Do one of the following actions:
   - If you selected **Update Content**, click **Yes**.
   - If you selected **Update Content and Scan**, select the type of scan, click **OK**, and then click **Yes**.

Chapter 9

Displaying features in the client user interface

This chapter includes the following topics:

About access to the client interface

You can determine the level of interaction that you want users to have on the Symantec Endpoint Protection client. Choose which features are available for users to configure. For example, you can control the number of notifications that appear and limit users' ability to create firewall rules and antivirus scans. You can also give users full access to the user interface.

The features that users can customize for the user interface are called managed settings. The user does not have access to all the client features, such as password protection.

To determine the level of user interaction, you can customize the user interface in the following ways:

- For antivirus and antispyware settings, you can lock or unlock the settings.
- For firewall settings, intrusion prevention settings, and for some client user interface settings, you can set the user control level and configure the associated settings.
- You can password-protect the client.

See "Password-protecting the client" on page 170.

Locking and unlocking managed settings

To determine which Antivirus and Antispyware Protection and Tamper Protection settings are available for users to configure on the client, you lock or unlock them. Users can configure unlocked settings, but users cannot configure locked settings. Only administrators in Symantec Endpoint Protection Manager can configure locked settings.

Table 9-1 Locked and unlocked padlock icons

Icon	What the icon means
	The setting is unlocked and users can change it in the client user interface. On the client, the padlock icon does not appear and the option is available.
	The setting is locked and users cannot change it in the client user interface. On the client, the locked padlock appears and the option appears dimmed.

You lock and unlock the settings on the pages or dialog boxes where they appear.

To lock and unlock managed settings

1. Open an Antivirus and Antispyware Policy.

   See "Editing a policy" on page 97.

2. On the Antivirus and Antispyware page, click one of the following pages:
   - File System Auto-Protect
   - Internet Email Auto-Protect
   - Microsoft Outlook Auto-Protect
   - Lotus Notes Auto-Protect
   - TruScan Proactive Threat Scans
   - Submissions
   - Miscellaneous

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

4 If you are finished with the configuration for this policy, click **OK**.

You can also lock and unlock Tamper Protection settings.

See "Configuring Tamper Protection" on page 380.

Changing the user control level

You can determine which Network Threat Protection features and client user interface settings are available for users to configure on the Symantec Endpoint Protection client. To determine which settings are available, you specify the user control level. The user control level determines whether the client can be completely invisible, display a partial set of features, or display a full user interface.

Note: The Symantec Network Access Control client only runs in server control. Users cannot configure any user interface settings.

Table 9-2 User control levels

User control level	Description
Server control	Gives the users the least control over the client. Server control locks the managed settings so that users cannot configure them. Server control has the following characteristics: ■ Users cannot configure or enable firewall rules, application-specific settings, firewall settings, intrusion prevention settings, or Network Threat Protection and Client Management logs. You configure all the firewall rules and security settings for the client in Symantec Endpoint Protection Manager. ■ Users can view logs, the client's traffic history, and the list of applications that the client runs. ■ You can configure certain user interface settings and firewall notifications to appear or not appear on the client. For example, you can hide the client user interface. The settings that you set to server control either appear dimmed or are not visible in the client user interface. When you create a new location, the location is automatically set to server control.

Table 9-2 User control levels *(continued)*

User control level	Description
Client control	Gives the users the most control over the client. Client control unlocks the managed settings so that users can configure them. Client control has the following characteristics: ■ Users can configure or enable firewall rules, application-specific settings, firewall notifications, firewall settings, intrusion prevention settings, and client user interface settings. ■ The client ignores the firewall rules that you configure for the client. You can give client control to the client computers that employees use in a remote location or a home location.
Mixed control	Gives the user a mixture of control over the client. Mixed control has the following characteristics: ■ Users can configure the firewall rules and application-specific settings. ■ You can configure the firewall rules, which may or may not override the rules that users configure. The position of the server rules in the Rules list of the firewall policy determines whether server rules override client rules. ■ You can specify certain settings to be available or not available on the client for users to enable and configure. These settings include the Network Threat Protection logs, Client Management logs, firewall settings, intrusion prevention settings, and some user interface settings. ■ You can configure Antivirus and Antispyware Protection settings to override the setting on the client, even if the setting is unlocked. For example, if you unlock the Auto-Protect feature and the user disables it, you can enable Auto-Protect. The settings that you set to client control are available to the user. The settings that you set to server control either appear dimmed or are not visible in the client user interface. See "About mixed control" on page 167.

Some managed settings have dependencies. For example, users may have permission to configure firewall rules, but cannot access the client user interface. Because users do not have access to the Configure Firewall Rules dialog box, they cannot create rules.

You can set a different user control level for each location.

Note: Clients that run in client control or mixed control switch to server control when the server applies a Quarantine Policy.

To change the user control level

1. In the console, click **Clients**.
2. Under View Clients, select the group whose location you want to modify.
3. Click the **Policies** tab.
4. Under Location-specific Policies and Settings, under the location you want to modify, expand **Location-specific Settings**.
5. To the right of Client User Interface Control Settings, click **Tasks > Edit Settings**.
6. In the Client User Interface Control Settings dialog box, do one of the following options:
   - Click **Server control**, and then click **Customize**.
     Configure any of the settings, and then click **OK**.
   - Click **Client control**.
   - Click **Mixed control**, and then click **Customize**.
     Configure any of the settings, and then click **OK**.
     See "About mixed control" on page 167.
   - For the Symantec Network Access Control client, you can click **Display the client** and **Display the notification area icon**.
7. Click **OK**.

About mixed control

For clients in mixed control, you can determine which managed options you want users to configure or not. Managed options include settings in a Firewall Policy, an Intrusion Prevention Policy, and the client user interface settings.

For each option, you can assign it to server control or you can assign it to client control. In client control, only the user can enable or disable the setting. In server control, only you can enable or disable the setting. Client control is the default user control level. If you assign an option to server control, you then configure the setting in the corresponding page or dialog box in the Symantec Endpoint Protection Manager console. For example, you can enable the firewall settings in

the Firewall Policy. You can configure the logs in the Client Log Settings dialog box on the Policies tab of the Clients page.

You can configure the following types of settings:

- User interface settings
  See "Configuring user interface settings" on page 168.
- General Network Threat Protection settings
  See "Configuring Network Threat Protection settings for mixed control" on page 499.
- Firewall Policy settings
  See "About working with Firewall Policies" on page 462.
- Intrusion Prevention Policy settings
  See "Configuring intrusion prevention" on page 486.

Configuring user interface settings

You can configure user interface settings on the client if you do either of the following tasks:

- Set the client's user control level to server control.
- Set the client's user control level to mixed control and set the parent feature on the Client/Server Control Settings tab to Server.
  For example, you can set the Show/Hide notification area icon option to Client. The notification area icon appears on the client and the user can choose to show or hide the icon. If you set the Show/Hide notification area icon option to Server, you can choose whether to display the notification area icon on the client.

To configure user interface settings in mixed control

1. Change the user control level to mixed control.

   See "Changing the user control level" on page 165.
2. In the Client User Interface Control Settings for *location name* dialog box, next to Mixed control, click **Customize**.
3. In the Client User Interface Mixed Control Settings dialog box, on the Client/Server Control Settings tab, do one of the following actions:
   - Lock an option so that you can configure it only from the server. For the option you want to lock, click **Server**.
     Any Antivirus and Antispyware Protection settings that you set to Server here override the settings on the client.

- Unlock an option so that the user can configure it on the client. For the option you want, click **Client**. Client is selected by default for all settings except the antivirus and antispyware settings.

4 For the following options that you set to Server, click the **Client User Interface Settings** tab to configure them:

Show/Hide notification area icon	Display the notification area icon
Enable/Disable Network Threat Protection	Allow users to enable and disable Network Threat Protection
Test Network Security menu command	Allow users to perform a security test
Configure unmatched IP traffic settings	Allow IP traffic or only application traffic, and prompt the user before allowing application traffic
Show/Hide Intrusion Prevention Notifications	Display Intrusion Prevention notifications

For information on where in the console you configure the remaining options that you set to Server, click **Help**. To enable firewall settings and intrusion prevention settings, configure them in the Firewall Policy and Intrusion Prevention Policy.

See "Enabling Smart traffic filtering" on page 479.

See "Enabling traffic and stealth settings" on page 480.

See "Configuring intrusion prevention" on page 486.

5 On the Client User Interface Settings tab, check the option's check box so that the option is available on the client.

6 Click **OK**.

7 Click **OK**.

To configure user interface settings in server control

1 Change the user control level to mixed control.

See "Changing the user control level" on page 165.

2 In the Client User Interface Control Settings for *location name* dialog box, next to Server control, click **Customize**.

3 In the Client User Interface Settings dialog box, check an option's check box so that the option appears on the client for the user to use.

4 Click **OK**.

5 Click **OK**.

Password-protecting the client

You can increase corporate security by requiring password protection on the client computer whenever users perform certain tasks.

You can require the users to type a password when users try to do one of the following actions:

- Open the client's user interface.
- Stop the client.
- Import and export the security policy.
- Uninstall the client.

You can modify password protection settings only for the subgroups that do not inherit from a parent group.

See "About access to the client interface" on page 163.

To password-protect the client

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

2 Under View Clients, select the group for which you want to set up password protection.

3 On the Policies tab, under Location-independent Policies and Settings, click **General Settings**.

4 Click **Security Settings**.

5 On the Security Settings tab, choose any of the following check boxes:

- Require a password to open the client user interface
- Require a password to stop the client service
- Require a password to import or export a policy
- Require a password to uninstall the client

6 In the Password text box, type the password.

The password is limited to 15 characters or less.

7 In the Confirm password text box, type the password again.

8 Click **OK**.

Chapter 10

Managing communication between management servers and clients

This chapter includes the following topics:

Managing the connection between management servers and clients

After you install the client, the management server automatically connects to the client computer. You can perform the following tasks to configure how the management server connects to clients.

If you have Symantec Network Access Control installed, you can also configure the connection between the management server and Enforcers.

Table 10-1 Tasks you can perform to manage connections between management servers and the clients

Task	Description
Read about management servers and management server lists	You can read about how management servers connect to clients. See "About management servers" on page 173.
Decide whether or not to use default management server list	You can add and then choose an alternative list of management servers then the default management server list. The management server list provides a list of multiple management servers that clients can connect to. See "Adding a management server list" on page 174. See "Specifying a management server list" on page 176. See "Changing the order in which management servers connect" on page 176.
Choose which method to download policies and content to the clients	You can configure the management server to push down policies to the client or for the clients to pull the policies from the management server. See "About updating policies on the clients" on page 108. See "Configuring push mode or pull mode to update client policies and content" on page 109.
Check the policy serial number in the client and in the management console	The policy serial number should match if the client can communicate with the server and receives regular policy updates. You can perform a manual policy update and then check the policy serial numbers against each other. See "Performing a manual policy update to check the policy serial number" on page 111.

Table 10-1 Tasks you can perform to manage connections between management servers and the clients *(continued)*

Task	Description
Configure communication settings for a location	You can configure separate communication settings for a location than a group. See "Configuring communication settings for a location" on page 182.
Check whether the client is connected to the management server	You can check the client status icon in the client and in the management console. The status icon shows whether the client and the server communicate. See "Viewing the client health state in the management console" on page 180. A computer may have the client software installed, but doesn't have the correct communications file. See "Converting an unmanaged client to a managed client" on page 66. See "Deploying client software with Find Unmanaged Computers" on page 125.
Troubleshoot connectivity problems with the management server	If the management server and the client do not connect, you can troubleshoot connection problems. See "Troubleshooting communication problems between the management server and the client" on page 183.

About management servers

Clients must be able to connect to management servers to download security policies and settings. The Symantec Endpoint Protection Manager includes a file that helps manage the traffic between clients and management servers. The file specifies to which management server a client connects. It can also specify to which management server a client connects in case of a management server's failure.

This file is referred to as a management server list. A management server list includes the management server's IP addresses or host names to which clients can connect after the initial installation. You can customize the management server list before you deploy any clients.

When the Symantec Endpoint Protection Manager is installed, a default management server list is created to allow for HTTP communication between clients and management servers. The default management server list includes

the IP addresses of all connected network interface cards (NICs) on all of the management servers at the site.

You may want to include only the external NICs in the list. Although you cannot edit the default management server list, you can create a customized management server list. A custom management server list includes the exact management servers and the correct NICs to which you want clients to connect. In a customized list, you can also use HTTPS protocol, verify the server certificate, and customize the HTTP or HTTPS port numbers.

Optionally, you can also use the management server list to specify to which server an optional Enforcer connects.

See "Configuring communication settings for a location" on page 182.

Adding a management server list

If your enterprise has multiple management servers, you can create a customized management server list. The management server list specifies the order in which clients in a particular group connect. Clients first try to connect to management servers that have been added with the highest priority.

If management servers with the highest priority are not available, then clients try to connect to management servers with the next higher priority. A default management server list is automatically created for each site. All available management servers at that site are added to the default management server list with the same priority.

If you add multiple management servers at the same priority, then clients can connect to any of the management servers. Clients automatically balance the load between available management servers at that priority.

You can use HTTPS protocol rather than the default HTTP for communication. If you want to secure communication further, you can customize the HTTP and HTTPS port numbers by creating a customized management server list. However, you must customize the ports before clients are installed or else the client-to-management server communication is lost. If you update the version of the management server, you must remember to re-customize the ports so that the clients can resume communication.

After you add a new management server list, you must assign it to a specific group or location or both.

See "Assigning a management server list to a group and location" on page 177.

To add a management server list

1. In the console, click **Policies**.
2. In the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
3. Under Tasks, click **Add a Management Server List**.
4. In the Management Server Lists dialog box, in the Name text field, type a name for the management server list and an optional description.
5. To specify which communication protocol to use between the management servers and the clients, select one of the following options:
   - Use HTTP protocol
   - Use HTTPS protocol
     Use this option if you want management servers to communicate by using HTTPS and if the server is running Secure Sockets Layer (SSL).
6. If you require verification of a certificate with a trusted third-party certificate authority, check **Verify certificate when using HTTPS protocol**.
7. To add a server, click **Add > New Server**.
8. In the Add Management Server dialog box, in the Server address text field, type the IP address or host name of the management server.
9. If you want to change the port number for either the HTTP or HTTPS protocol for this server, do one of the following tasks:
   - Check **Customize HTTP port number** and enter a new port number.
     The default port number for the HTTP protocol is 8014.
   - Check **Customize HTTPS port number** and enter a new port number.
     The default port number for the HTTPS protocol is 443.
     If you customize the HTTP or HTTPS port numbers after client deployment, clients lose communication with the management server.
10. Click **OK**.
11. If you need to add a management server that has a different priority than the management server you just added, click **Add > New Priority**.
12. Repeat steps 7 through 10 to add more management servers.
13. In the Management Server Lists dialog box, click **OK**.

Specifying a management server list

You can specify a list of management servers to connect to a group of clients and optional Enforcers at any time. However, you typically perform this task after you have created a custom management server list and before you deploy any client packages.

See "Adding a management server list" on page 174.

To specify a management server list

1. In the console, click **Clients**.
2. On the Clients page, under View Clients, select the group for which you want to specify a management server list.
3. On the Policies tab, uncheck **Inherit policies and settings from parent group**.

   You cannot set any communication settings for a group unless the group no longer inherits any policies and settings from a parent group.
4. Under Location-independent Policies and Settings, in the Settings area, click **Communication Settings**.
5. In the Communication Settings for *group name*, under Management Server List, select the management server list.

   The group that you select then uses this management server list when communicating with the management server.
6. Click **OK**.

Changing the order in which management servers connect

If circumstances change in a network, you may need to reassign IP addresses or host names, as well as priorities in a management server list. For example, one of the servers on which you installed the Symantec Endpoint Protection Manager had a disk failure. This management server had served as a load balancing server and had been assigned Priority 1. However, you have another management server with an assigned Priority 2. If you want to resolve this problem, you can reassign the priority of this management server. You can assign a management server's priority from 2 to 1 to replace the defective management server.

See "Adding a management server list" on page 174.

To change the order in which management servers connect

1. In the console, click **Policies**.
2. On the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
3. In the Management Server Lists pane, select the management server list for which you want to change the order of the management servers.
4. Under Tasks, click **Edit the List**.
5. In the Management Server Lists dialog box, under Management Servers, select the IP address, host name, or priority of the management server.

   You can move an IP address or a host name to a different priority. If you decide to change a priority, it also automatically changes the priority of all of the associated IP addresses and host names.
6. Click **Move Up** or **Move Down**.
7. In the Management Server Lists dialog, click **OK**.

Assigning a management server list to a group and location

After you add a policy, you need to assign it to a group or a location or both. Otherwise the management server list is not effective. You can also use the management server list to move a group of clients from one management server to another.

You must have finished adding or editing a management server list before you can assign the list.

See "Adding a management server list" on page 174.

To assign a management server list to a group and location

1. In the console, click **Policies**.
2. In the Policies page, under View Policies, click **Policy Components > Management Server Lists**.
3. In the Management Server Lists pane, select the management server list you want to assign.
4. Under Tasks, click **Assign the List**.
5. In the Apply Management Server List dialog box, check the groups and locations to which you want to apply the management server list.

6 Click **Assign**.

7 When you are prompted, click **Yes**.

Viewing the groups and locations to which a management server list is assigned

You may want to display the groups and locations to which a management server list has been assigned.

See "Assigning a management server list to a group and location" on page 177.

To view the groups and locations to which a management server list is assigned

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

2 On the Policies page, under View Policies, click **Policy Components > Management Server Lists**.

3 In the Management Server Lists pane, select the management server list whose groups and locations you want to display.

4 Under Tasks, click **Show the Assigned Groups or Locations**.

The groups or locations that are assigned the selected management server list display a small green circle with a white check mark.

5 In the *management server list name*: Assigned Groups & Locations dialog box, click **OK**.

Replacing a management server list

You may want to replace a management server list that has previously been applied to a specific group or location with another one.

See "Adding a management server list" on page 174.

To replace a management server list

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

2 On the Policies page, under View Policies, click **Policy Components > Management Server Lists**.

3 In the Management Server Lists pane, select the management server list that you want to replace.

4 Under Tasks, click **Replace the List**.

5 In the Replace Management Server List dialog box, select the replacement management server list from the New Management Server drop-down list.

6 Check the groups or locations to which you want to apply the replacement management server list.

7 Click **Replace**.

8 When you are prompted, click **Yes**.

Copying and pasting a management server list

You may want multiple management lists that are nearly identical, except for a few changes. You can make a copy of a management server list. After you copied and pasted a management server list, the copy of the management server list appears in the Management Server Lists pane.

See "Adding a management server list" on page 174.

To copy and paste a management server list

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

2 On the Policies page, under View Policies, click **Policy Components > Management Server Lists**.

3 In the Management Server Lists pane, select the management server list that you want to copy.

4 Under Tasks, click **Copy the List**.

5 Under Tasks, click **Paste List**.

Exporting and importing a management server list

You may want to export or import an existing management server list. Server lists are often used when setting up replication between servers. The file format for a management server list is: .dat

See "Adding a management server list" on page 174.

To export a management server list

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

2 On the Policies page, under View Policies, click **Policy Components > Management Server Lists**.

3 In the Management Server Lists pane, select the management server list that you want to export.

4 On the Policies page, under Tasks, click **Export the List**.

5 In the Export Policy dialog box, browse for the folder into which you want to export the management server list file.

6 Click **Export**.

7 If you are prompted to change the file name in the Export Policy dialog, modify the file name, and then click **OK**.

To import a management server list

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

2 In the Policies page, under View Policies, click **Policy Components > Management Server Lists**.

3 Under Tasks, click **Import a Management Server List**.

4 In the Import Policy dialog box, browse to the management server list file that you want to import, and then click **Import**.

5 If you are prompted to change the file name in the Input dialog box, modify the file name, and then click **OK**.

Viewing the client health state in the management console

You can check the client status icon in the management console as well as on the client directly to determine client status.

Table 10-2 Client status icons in the management console

Icon	Description
	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode.
	This icon indicates the following status: ■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client may have been added from the console, and may not have any Symantec client software installed.

Table 10-2 Client status icons in the management console *(continued)*

Icon	Description
	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client is an unmanaged detector.
	This icon indicates the following status: ■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client is an unmanaged detector.
	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in user mode.
	This icon indicates the following status: ■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in user mode. ■ The client may have been added from the console, and may not have any Symantec client software installed.
	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in computer mode.
	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in computer mode. ■ The client is an unmanaged detector.
	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in user mode.

See "What you can do from the console" on page 40.

To view the client health status in the management console

1. In the management console, on the Clients page, under View Clients, select the group in which the client belongs.
2. Look on the Clients tab.

   The client name should appear in the list next to an icon that shows the client status.

Configuring communication settings for a location

By default, you configure the same communication settings between the management server and the client for all the locations within a group. However, you can also configure these settings for each location separately. For example, you can use a separate management server for a location where the client computers connect through the VPN. Or, to minimize the number of clients that connect to the management server at the same time, you can specify a different heartbeat for each location.

See "Configuring push mode or pull mode to update client policies and content" on page 109.

You can configure the following communication settings for locations:

The following settings are specific to locations:

- The control mode that the clients run in.
- The management server list that the clients use.
- The download mode that the clients run in.
- Whether or not you want a list of all the applications that are executed on clients to be collected and sent to the management server.
- The heartbeat interval that clients use for downloads.
- Whether or not the management server randomizes content downloads from the default management server or a Group Update Provider.

To configure communication settings for a location

1. In the console, click **Clients**.
2. On the **Clients** page, select a group.
3. On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.

4 To the right of **Communications Settings**, click **Tasks**, and then uncheck **Use Group Communications Settings**.

5 Click **Tasks** again, and then click **Edit Settings**.

6 In the **Communications Settings for *location name*** dialog box, modify the settings for that location only.

7 Click **OK**.

Troubleshooting communication problems between the management server and the client

If you have trouble with client and server communication, you should first check to make sure that there are no network problems. You should also check network connectivity before you call Symantec Technical Support.

You can test the communication between the client and the management server in several ways.

Table 10-3 Checking the connection between the management server and the client

What to check	Description
View the communication settings on the client	You can download and view the troubleshooting file on the client to verify the communication settings. See "Investigating client problems" on page 184.
Test the connectivity between the client and the management server	You can issue several commands on the client to test the connectivity to the management server. You can do the following tests: ■ Ping the management server from the client computer. See "Using the ping command to test the connectivity to the management server" on page 185. ■ Telnet to the management server from the client computer. See "Using Telnet to test the connectivity to the management server" on page 186. ■ Use a Web browser on the client computer to connect to the management server. See "Using a browser to test the connectivity to the management server" on page 185.

Table 10-3 Checking the connection between the management server and the client *(continued)*

What to check	Description
Check for any network problems	You should verify that there are no network problems by checking the following items: ■ Test the connectivity between the client and management server first. If the client computer cannot ping or Telnet to the management server, you should verify the DNS service for the client. ■ Check the client's routing path. ■ Check that the management server does not have a network problem. ■ Check that the Symantec Endpoint Protection firewall (or any third-party firewall) does not cause any network problems.
Check the IIS logs on the management server	You can check the IIS logs on the management server. The logs can help you to determine whether the client can communicate with the IIS server on the management server computer. See "Checking the IIS logs on the management server" on page 188.
Check the debug logs on the client	You can use the debug log on the client to determine if the client has communication problems. See "Checking the debug log on the client computer" on page 187.
Recover lost client communication	If the clients have lost the communication with a management server, you can use a tool to recover the communication file. See "Recovering client communication settings by using the SylinkDrop tool" on page 188.

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.

See "Troubleshooting communication problems between the management server and the client" on page 183.

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.

Using the ping command to test the connectivity to the management server

You can try to ping the management server from the client computer to test connectivity.

See "Troubleshooting communication problems between the management server and the client" on page 183.

To use the ping command to test the connectivity to the management server

1. On the client, open a command prompt.
2. Type the ping command. For example:

   ping *name*

   where *name* is the computer name of the management server. You can use the server IP address in place of the computer name. In either case, the command should return the server's correct IP address.

   If the ping command does not return the correct address, verify the DNS service for the client and check its routing path.

Using a browser to test the connectivity to the management server

You can use a Web browser to test the connectivity to the management server.

See "Troubleshooting communication problems between the management server and the client" on page 183.

To use a browser to test the connectivity to the management server

1. On the client computer open a Web browser, such as Internet Explorer.
2. In the browser command line, type a command that is similar to either of the following commands:

   http://*management server IP address*:8014/reporting/index.php

   If the reporting logon Web page appears, the client can communicate with the management server.

   http://*management server name*:8014/secars/secars.dll?secars,hello

   If the Symantec Endpoint Protection Manager page appears, the client can communicate with the management server.
3. If a Web page does not appear, check for any network problems. Verify the DNS service for the client and check its routing path.

Using Telnet to test the connectivity to the management server

You can use Telnet to test the connectivity to the IIS server on the management server. If the client can Telnet to the management server's HTTP or HTTPS port, the client and the server can communicate. The default HTTP port is 80; the default HTTPS port is 443.

Note: You might need to adjust your firewall rules so that the client computer can Telnet into the management server.

See "Troubleshooting communication problems between the management server and the client" on page 183.

To use Telnet to test the connectivity to the management server

1. On the client computer, make sure the Telnet service is enabled and started.
2. Open a command prompt and enter the Telnet command. For example:

   telnet *ip address* 80

   where *ip address* is the IP address of the management server.

   If the Telnet connection fails, verify the client's DNS service and check its routing path.

Checking the debug log on the client computer

You can check the debug log on the client. If the client has communication problems with the management server, status messages about the connection problem appear in the log.

See "Troubleshooting communication problems between the management server and the client" on page 183.

You can check the debug log by using the following methods:

- In the client, on the Help and Support menu, in the Troubleshooting dialog box, you can click **Edit Debug Log Settings** and type a name for the log. You can then click **View Log**.
- You can use the Windows registry to turn on debugging in the client. You can find the Windows registry key in the following location: HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\smc_debuglog_on

Checking the inbox logs on the management server

You can use a Windows registry key to generate logs about activity in the management server inbox.

When you modify the Windows registry key, the management server generates the logs (ersecreg.log and exsecars.log). You can view these logs to troubleshoot client and server communication. You can find the logs in the log directory of the inbox on the management server.

See "Troubleshooting communication problems between the management server and the client" on page 183.

To check the inbox logs on the management server

- On the management server, under HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM, set the DebugLevel value to 3.

  Typically, the inbox appears in the following location on the management server computer:

  ```
  \Program Files\Symantec\Symantec Endpoint Protection Manager\data\
  inbox\log
  ```

  You can open the logs with a text application such as Notepad.

Checking the IIS logs on the management server

You can check the IIS logs on the management server. The logs show GET and POST commands when the client and the server communicate.

See "Troubleshooting communication problems between the management server and the client" on page 183.

To check the IIS logs on the management server

1. On the management server, go to the IIS log files directory. A typical path to the directory is:

   \WINDOWS\system32\LogFiles\W3SVC1

2. Open the most recent log file with a text application such as Notepad. For example, the log file name might be ex070924.log.

3. Review the log messages.

   The file should include both GET and POST messages.

Recovering client communication settings by using the SylinkDrop tool

The Sylink.xml file includes communication settings between the client and a Symantec Endpoint Protection Manager server. If the clients have lost the communication with a management server, you must replace the old Sylink.xml file with a new file. The SylinkDrop tool automatically replaces the Sylink.xml file on the client computer with a new Sylink.xml file.

When you run the SylinkDrop tool, it can also perform the following tasks:

- Migrates or moves clients to a new domain or management server.
- Restores the communication breakages to the client that cannot be corrected on the management server.
- Moves a client from one server to another server that is not a replication partner.
- Moves a client from one domain to another.
- Converts an unmanaged client to a managed client.
- Converts a managed client to an unmanaged client.

You can use write a script with the tool to modify communication settings for large numbers of clients.

See "Troubleshooting communication problems between the management server and the client" on page 183.

To recover client communication settings by using the SylinkDrop tool

1. In the console, export the communication file from the group that connects to the management server to which you want the client computer to connect.

   See "Converting an unmanaged client to a managed client" on page 66.

2. Deploy the communication file to the client computer.
3. On Disk 3 of the installation CD, locate the \Tools\NoSupport\SylinkDrop folder, and open SylinkDrop.exe.

   You can run the tool remotely or save it and then run it on the client computer. If you use the tool on the command line, read the SylinkDrop.txt file for a list of the tool's command parameters.

4. In the Sylink Drop dialog box, click **Browse**, and locate the .xml file you deployed in step 2 to the client computer.
5. Click **Update Sylink**.
6. If you see a confirmation dialog box, click **OK**.
7. In the Sylink Drop dialog box, click **Exit**.

Chapter 11

Monitoring endpoint protection

This chapter includes the following topics:

Monitoring endpoint protection

Symantec Endpoint Protection and Symantec Network Access Control collect information about the security events in your network. You can use log and reports to view these events, and you can use notifications to stay informed about the events as they occur.

You can perform the following tasks on Symantec Endpoint Protection Manager to protect the computers in your network.

Table 11-1 Tasks for monitoring endpoint protection

Task	Description
Monitor the security status of your network	You can view information on the distribution of virus definitions, links to Symantec Security Response, and links to your favorite reports. You can perform the following tasks to obtain the security status of the client computers ■ Obtain a count of detected viruses and other security risks and view details for each virus and security risk. See "About the Symantec Endpoint Protection Home page" on page 198. ■ View a graph of risks, attacks, or infections per hour ■ Obtain a count of unprotected computers in your network and view details for each. ■ View virus definitions distribution and intrusion prevention distribution for the last 12 hours. Also, view the dates of the latest version of definitions from Symantec and on Symantec Endpoint Protection Manager. ■ View a summary of how many client computers are protected See "Using the Monitors Summary tab" on page 208.
Review which client computers need protection	You can do the following tasks to view which computers need additional protection: ■ View event logs. See "About logs" on page 261. See "Viewing logs" on page 267. ■ Run predefined and customizable reports with data that the management server collects from the clients. See "About reporting" on page 196. See "Creating quick reports" on page 250. ■ Schedule reports on the security status to be emailed regularly to other administrators See "Creating and deleting scheduled reports" on page 255.

Table 11-1 Tasks for monitoring endpoint protection *(continued)*

Task	Description
Protect your client computers	You can issue commands from the console to protect the client computers. ■ Eliminate security risks on client computers See "Eliminating viruses and security risks" on page 214. ■ View which clients are offline. See "Finding the clients that are offline" on page 218. ■ Run commands on the client from the console See "Running commands and actions from logs" on page 274.
Configure notifications to alert you when security events occur	You can create and configure notifications to be triggered when certain security-related events occur. For example, you can set a notification to occur when an intrusion attempt occurs on a client computer. See "About using notifications" on page 281. See "Viewing and filtering administrator notification information" on page 281. See "Creating administrator notifications" on page 283.

About different methods of accessing the reporting functions

Reporting runs as a Web application within the Symantec Endpoint Protection Manager console. The application uses a Web server to deliver this information. You can access the reporting functions, which are located on the Home page, Monitors page, and Reports page, from the console.

You can also access the Home, Monitors, and Reports page functions from a stand-alone Web browser that is connected to your management server. You can perform all the reporting functions from either the console or a stand-alone Web browser. However, all of the other console functions are not available when you use a stand-alone browser.

Note: The information that is provided in this document assumes that you use the console to access reporting functions rather than a Web browser. Procedures for using the reporting functions are similar regardless of how you access reporting. However, procedures specific to how you use reporting in a stand-alone browser are not documented, except for how to log on using a stand-alone Web browser.

See "Logging on to reporting from a stand-alone Web browser" on page 194.

See "Logging on to the Symantec Endpoint Protection Manager console" on page 37.

To access the reporting functions by either method, you must have Internet Explorer 6.0 or later installed. Other Web browsers are not supported.

Also, you can also use the console or a Web browser to view reports when logged in through a remote terminal session. Report pages and log pages always display in the language that the management server was installed with. To display these pages when you use a remote console or browser, you must have the appropriate font installed on the computer that you use.

To access reporting from a Web browser, you must have the following information:

- The IP address or host name of the management server.
- The account name and password for the manager.

When you use a Web browser to access reporting functions, no pages or page icons are in the display. All the tabs that are located on the Home, Monitors, and Reports console pages are located across the top of the browser window.

You can access context-sensitive Help by clicking the **Tell me more** link, which is located on the console pages that are used for reporting functions.

See "Changing the port used to access context-sensitive help for reporting" on page 195.

Logging on to reporting from a stand-alone Web browser

You can access the Home, Monitors, and Reports page functions from a stand-alone Web browser that is connected to your management server. You can perform all the reporting functions from a stand-alone Web browser. However, all of the other console functions are not available when you use a stand-alone browser.

Note: You must have Internet Explorer 6.0 or later installed. Other Web browsers are not supported.

See "About different methods of accessing the reporting functions" on page 193.

To log on to reporting from a stand-alone Web browser

1. Open a Web browser.
2. Type the reporting URL into the address text box in the following format:

   http://*server name*:*port* /reporting/index.php?
3. When the logon dialog box appears, type your user name and password, and then click **Log On**.

   If you have more than one domain, in the **Domain** text box, type your domain name.

Changing the port used to access context-sensitive help for reporting

If you do not use the default port when you install the Help pages for reporting, you cannot access the on-line context-sensitive help. To access context-sensitive help when you use a non-default port, you must add a variable to the Reporter.php file.

See "About different methods of accessing the reporting functions" on page 193.

To change the port used to access context-sensitive help for reporting

1. Change directory to *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\Reporting\Resources.
2. Open the Reporter.php configuration file with an editor.
3. Add the following line to the file, and replace *port number* with the port number you used when you installed reporting Help.

   $scm_http_port=*port number*
4. Save and close the file.

Associating localhost with the IP address when loopback addresses is disabled

If you have disabled loopback addresses on the computer, the reporting pages do not display. If you try to log on to the Symantec Endpoint Protection Manager console or to access the reporting functions, you see the following error message:

Unable to communicate with Reporting component

The **Home**, **Monitors**, and **Reports** pages are blank; the **Policies**, **Clients**, and **Admin** pages look and function normally.

To get the **Reports** components to display when you have disabled loopback addresses, you must associate the word localhost with your computer's IP address. You can edit the Windows hosts file to associate localhost with an IP address.

See "About different methods of accessing the reporting functions" on page 193.

To associate localhost with the IP address on computers running Windows

1. Change directory to the location of your hosts file.

   By default, the hosts file is located in *%SystemRoot%*\system32\drivers\etc

2. Open the hosts file with an editor.

3. Add the following line to the hosts file:

   xxx.xxx.xxx.xxx **localhost** #*to log on to reporting functions*

   where you replace *xxx.xxx.xxx.xxx* with your computer's IP address. You can add any comment you want after the pound sign (#). For example, you can type the following line:

   192.168.1.100 localhost # this entry is for my console computer

4. Save and close the file.

About reporting

The reporting functions give you the up-to-date information that you need to monitor and make informed decisions about the security of your network.

The Symantec Endpoint Protection Manager console **Home** page displays the automatically generated charts that contain information about the important events that have happened recently in your network.

You can use the filters on the **Reports** page to generate predefined or custom reports. You can use the **Reports** page to view graphical representations and statistics about the events that happen in your network. You can use the filters on the **Monitors** page to view more detailed, real-time information about your network from the logs.

Table 11-2 Reporting tasks

Task	Description
Monitor your security status using the Home page (Symantec Endpoint Protection and Symantec Network Access Control)	If you have Symantec Endpoint Protection installed, the **Home** page shows your security status, information on distribution of virus definitions, links to Symantec Security Response, and links to your favorite reports. See "About the Symantec Endpoint Protection Home page" on page 198. If you have Symantec Network Access Control installed, reporting includes a Home page with an overall summary view of compliance status. See "Using the Symantec Network Access Control Home page" on page 207.
Generate quick reports (Symantec Endpoint Protection and Symantec Network Access Control)	Predefined quick reports and customizable graphical reports with multiple filter options that you can configure See "About quick reports" on page 246.
Generate scheduled reports (Symantec Endpoint Protection and Symantec Network Access Control)	The ability to schedule reports to be emailed to recipients at regular intervals See "About scheduled reports" on page 254.
View summary reports (Symantec Endpoint Protection only)	Summary views of reports that show status on Antivirus and TruScan Proactive Threat, Network Threat Protection, Compliance, and Site Status See "Using the Monitors Summary tab" on page 208.

Reporting runs as a Web application within the console. The application uses a Web server to deliver this information. You can also access reporting functions from a stand-alone Web browser that is connected to your management server.

See "About different methods of accessing the reporting functions" on page 193.

See "About the reports you can run" on page 221.

About logged events from your network

Symantec Endpoint Protection pulls the events that appear in the reports from the event logs on your management servers. The event logs contain time-stamps in the clients' time zones. When the management server receives the events, it converts the event time-stamps to Greenwich Mean Time (GMT) for insertion into

the database. When you create reports, the reporting software displays information about events in the local time of the computer on which you view the reports.

Some types of events such as virus outbreaks can generate an excessive number of security events. These types of events are aggregated before they are forwarded to the management server. You can reduce the number of events that are sent to the antivirus and antispyware logs by configuring log handling parameters. These options are configured on a per-policy basis from your Antivirus and Antispyware Policy.

See "Setting up log handling parameters in an Antivirus and Antispyware Policy" on page 409.

For information about the events that appear on the **Home** page, see the **Symantec Security Response** Web site, **Attack Signatures** page. On the Internet, go to the following URL:

http://securityresponse.symantec.com/business/security_response/attacksignatures/index.jsp

How reporting uses the logs stored in the database

Symantec Endpoint Protection collects and reads the events that occur in your network from the management server logs stored in the database. The database can be an existing Microsoft SQL database in your network or the embedded database that is installed with the reporting software.

The database has a few reporting-related maintenance requirements.

See "About managing log events in the database" on page 365.

You can obtain the database schema that Symantec Endpoint Protection uses if you want to construct your own reports by using third-party software. For information about the database schema, download the latest *Database Schema Reference* from the Symantec Endpoint Protection documentation site.

About the Symantec Endpoint Protection Home page

If you have Symantec Endpoint Protection installed and your administrator account rights include permission to view reports, then your Home page displays automatically generated reports. These reports contain important information about your network security. If you do not have permission to view reports, your **Home** page does not contain these automatically generated reports.

The Home page includes automatically generated reports and several status items. Some of the Home page reports are hyperlinked to more detailed reports. You can click on the numbers and some charts in the Home page reports to see details.

Note: Reports are filtered automatically based on the permissions of the user who is logged on. If you are a system administrator, you see information across domains. If you are a limited administrator with access rights to only one domain, you see information from only that one domain.

Table 11-3 describes each item on the Symantec Endpoint Protection Home page in detail.

Table 11-3 Home page items and reports

Report or Status Information	Description
Security Status	**Security Status** can be either **Good** or **Attention Needed**. The thresholds that you set on the **Security Status** tab determine the definitions of **Good** and **Attention Needed**. You access the **Security Status** tab from the **Preferences** link on the **Home** page. See "Configuring security status thresholds" on page 212. You can click the security status icon on the **Home** page for details.

Table 11-3 Home page items and reports *(continued)*

Report or Status Information	Description
Action Summary by Detection Count | *Action Summary by Number of Computers*	By default, the **Home** page displays an action summary for the last 24 hours and by the infection count for viruses and security risks. You can click the Preferences link to change the time interval that is used to the past week instead of the past 24 hours. You can use the same link to change the display by Detection Count to a display by the Number of Computers. See "About Home and Monitors display options" on page 211. The Action Summary by Detection Count summarizes the following information: ■ A count of the actions that have been taken on viruses and security risks. ■ The incidence of new virus and security risk detections. ■ The number of computers that remain infected by viruses and security risks. The Action Summary by Number of Computers summarizes the following information: ■ The number of distinct computers on which the various actions have been performed on viruses and security risks. ■ The total number of new virus and security risk detections. ■ The total number of computers that still remain infected by viruses and security risks. For example, suppose you have five Cleaned actions in the Detection Count view. If all of the detections occur on the same computer, then the Number of Computers view shows a count of one, not five. For any of the actions, click the number of viruses or security risks to see a detailed report. A suspicious security risk indicates that a **TruScan proactive threat scan** has detected something that you should investigate. It may or may not be harmless. If you determine that this risk is harmless, you can use the Centralized Exceptions Policy to exclude it from detection in the future. If you have configured TruScan proactive threat scans to log, and you determine that this risk is harmful, you can use the Centralized Exceptions Policy to terminate or quarantine it. If you have used the default **TruScan proactive threat scan** settings, then Symantec Endpoint Protection cannot remediate this risk. If you determine that this risk is harmful, you should remove the risk manually.

Table 11-3 Home page items and reports *(continued)*

Report or Status Information	Description
Action Summary by Detection Count | *Action Summary by Number of Computers* (Continued)	The Newly Infected count shows the number of risks that have infected computers during the selected time interval only. Newly Infected is a subset of Still Infected. The Still Infected count shows the total number of risks that a scan would continue to classify as infected, also within the configured time interval. For example, computer may still be infected because Symantec Endpoint Protection can only partially remove the risk. After you investigate the risk, you can clear the Still Infected count from the Computer Status log. Both the Newly Infected count and the Still Infected count show the risks that require you to take some further action to clean. In most cases, you can take this action from the console and do not have to go to the computer. **Note:** A computer is counted as part of the Newly Infected count if the detection event that occurred during the time range of the Home page. For example, if an unremediated risk affected a computer within the past 24 hours, the Newly Infected count goes up on the Home page. The risk can be unremediated because of a partial remediation or because the security policy for that risk is set to Log Only. You can configure a database sweep to remove or retain the detection events that resulted in unremediated risks. If the sweep is configured to remove the unremediated risk events, then the Home page count for Still Infected no longer contains those events. Those events age out and are dropped from the database. This disappearance does not mean that the computers have been remediated. No time limit applies to Still infected entries. After you clean the risks, you can change the infected status for the computer. Change the status in the Computer Status log by clicking the icon for that computer in the Infected column. **Note:** The Newly Infected count does not decrement when a computer's infection status is cleared in the Computer Status log; the Still Infected count does decrement. You can determine the total number of events that have occurred in the last time period configured to show on the Home page. To determine total number, add the counts from all rows in the Action Summary except for Still Infected. See "Viewing logs" on page 267.

Table 11-3 Home page items and reports *(continued)*

Report or Status Information	Description
Attacks | *Risks* | *Infections Per Hour: Last 12 Hours* | *Per Hour: Last 24 Hours*	This report consists of a line graph. The line graph demonstrates the incidence of either the attacks, detections, or infections in your security network over the last 12 hours or 24 hours. You can select one of the following choices to display: ■ Attacks represent the incidents that Network Threat Protection thwarted. ■ Risks represent all the antivirus, antispyware, and **TruScan proactive threat scan** detections that were made. ■ Infections represent the viruses and security risks that were detected, but cannot be properly remediated. You can change the display by clicking a new view in the list box. **Note:** You can click the Preferences link to change the default time interval that is used. See "About Home and Monitors display options" on page 211.
Notification status summary	The Notification status summary shows a one-line summary of the status of the notifications that you have configured. For example, 100 unacknowledged notifications in the last 24 hours. See "Creating administrator notifications" on page 283.
Status Summary	The Status Summary summarizes the operational state of the computers in your network. It contains the number of computers in the network that have the following problems: ■ The Antivirus Engine is turned off. ■ Auto-Protect is turned off. ■ Tamper Protection is turned off. ■ The computers require a restart to complete some form of risk remediation or to complete the installation of a LiveUpdate software download. ■ The computers have failed a Host Integrity check. This number is always zero if you do not have Symantec Network Access Control installed. ■ The computers that have not checked in with the management server. You can click each number under **Computers** to view the details. Also, the number of unacknowledged notifications in the last 24 hours appears as a link below the **Status Summary**. Click the link to open the **Notifications** window. See "Viewing and filtering administrator notification information" on page 281.

Table 11-3 Home page items and reports *(continued)*

Report or Status Information	Description
Virus Definitions Distribution | *Intrusion Prevention Signatures*	The **Virus Definitions Distribution** and **Intrusion Prevention Signature Distribution** section of the **Home** page shows how the current virus definitions and IPS signatures are distributed. You can toggle between them by clicking a new view in the list box.
Security Response	The Security Response section shows the Top Threats and the Latest Threats as determined by Symantec Security Response. It also shows the number of computers in your network that are unprotected from these threats. The ThreatCon meter indicates the current severity level of threat to computers in a network. The severity levels are based on the threat assessments that Symantec Security Response makes. The ThreatCon severity level provides an overall view of global Internet security. You can click any of the links to get additional information. See "About using Security Response links" on page 205. **Note:** Symantec does not support the installation of the Symantec Client Firewall on the same computer as the Symantec Endpoint Protection Manager. If you install both on the same computer, this situation can cause CGI errors when you click the Security Response links on the Home page.
Watched Applications Summary	The Watched Applications Summary shows the occurrences of applications in your network that are on the following lists: ■ The **Commercial Application Detection** list ■ The **Forced TruScan Proactive Threat Detection** list, which is your custom list of watched applications You can click a number to display a more detailed report.
Favorite Reports	The Favorite Reports section contains three default reports. You can customize this section by replacing one or more of these reports with any other default report or custom report that you want. Favorite reports run every time you view them so that their data is current. They display in a new window. To select the reports that you want to access from the Home page, you can click the plus icon beside Favorite Reports. See "Configuring the Favorite Reports on the Home page" on page 204.

You can click **Preferences** under **Security Status** to change the time period for the reports and the summaries that display on those pages. The default is the past 12 hours; the other option is the past 24 hours. You can also change the default reports that are displayed in the Favorite Reports section of the Home page.

Configuring the Favorite Reports on the Home page

You can configure the Favorite Reports section on the Home page to provide links to up to three reports that you want to see regularly. You can use this feature to display the reports that you want to see most frequently, every time you log on to the Symantec Endpoint Protection Manager console. The Favorite Reports run every time you view them, so they display current information about the state of your network.

The following reports appear in Favorite Reports by default:

- Top Sources of Attack
- Top Risk Detections Correlation
- TruScan Proactive Threat Distribution

Note: When you customize the display, you customize the display for the currently logged-on user account only.

The settings that you configure on this page are saved across sessions. The next time you log on to the console with the same user credentials, these settings are used for the Home page display.

Table 11-4 describes the Home page display options.

Table 11-4 Home page favorite reports display options

Option	Definition
Report Type	Specifies the types of reports that are available. Symantec Endpoint Protection provides the following types of reports: ■ Application and Device Control ■ Audit ■ Compliance ■ Computer Status ■ Network Threat Protection ■ Risk ■ Scan ■ System
Report Name	Lists the names of the reports available for the type of report you selected.

Table 11-4 Home page favorite reports display options *(continued)*

Option	Definition
Filter	If you have saved filters associated with the report you selected, they appear in this list box. The default filter is always listed.

See "About the Symantec Endpoint Protection Home page" on page 198.

To configure the favorite reports on the Home page

1. Click **Home**.
2. Click the plus icon beside **Favorite Reports**.
3. From the list box of the report that you want to change, click a report type. For example, click **Risk**.
4. From the next list box, click the report name you want. For example, click **Risk Distribution Over Time**.
5. If you have saved filters associated with the report you selected, select the one you want to use or select the default filter.
6. Repeat for the second and third report links, if desired.
7. Click **OK**.

   Links to the reports that you selected appear on your Home page.

About using Security Response links

The Home page includes a summary that is based on the information from the Symantec Security Response Web site. The ThreatCon level severity chart appears as well as links to the Symantec Security Response Web site and other security Web sites. The ThreatCon level shows the condition of the Internet during the last 24 hours. The level is reevaluated every 24 hours unless Internet activity is such that it needs to be done sooner.

The ThreatCon levels are as follows:

- 1 - Normal
  No discernible network incident activity and no malicious code activity with a moderate or severe risk rating. Under Normal conditions, only a routine security posture, designed to defeat normal network threats, is needed. Automated systems and notification mechanisms should be used.
- 2 - Elevated
  The knowledge or the expectation of attack activity is present, without the occurrence of specific events. This rating is used when malicious code reaches

a moderate risk rating. Under this condition, a careful examination of vulnerable and exposed systems is appropriate. Security applications should be updated with new signatures and rules as soon as they become available. The careful monitoring of logs is recommended, but no change to actual security infrastructure is required.

- 3 - High
  This level applies when an isolated threat to the computing infrastructure is currently underway or when malicious code reaches a severe risk rating. Under this condition, increased monitoring is necessary. Security applications should be updated with new signatures and rules as soon as they become available. The redeployment and reconfiguration of security systems is recommended.
- 4 - Extreme
  This level applies when extreme global network incident activity is in progress. Implementation of measures in this Threat Condition for more than a short period might create hardship and affect the normal operations of network infrastructure.

For more information about the threat levels, click the Symantec link to display the Symantec Web site.

Note: Specific security risks are rated from 1 to 5.

Each link displays a page in a new window.

Table 11-5 describes the Security Response links.

Table 11-5 Security Response links on the reporting Home page

Link	What displays
Security Alerts	Displays a summary of the potential threats to your security network that is based on information from Symantec Security Response. The summary includes the latest threats, top threats, and links to removal tools. You can also search the Symantec Security Response threat database.
Symantec	Displays the Symantec Web site. You can get information about risks and security risks, virus definition downloads, and recent news about Symantec security products.
Definitions	Displays the virus definition download page of the Symantec Web site.

Table 11-5 Security Response links on the reporting Home page *(continued)*

Link	What displays
Latest Threats	Displays the Symantec Security Response Web site, which shows the latest threats and security advisories.
Security Focus	Displays the Security Focus Web site, which shows information about the latest viruses.

See "About the Symantec Endpoint Protection Home page" on page 198.

Using the Symantec Network Access Control Home page

If you have Symantec Network Access Control installed, and you have permission to view reports, then your **Home** page displays automatically generated summaries. These reports contain important information about network compliance status. Some of the summaries are hyperlinked to more detailed reports. You can click on the chart and the numbers in the summaries to see details.

Note: Reports are filtered automatically based on the permissions of the user who is logged on. If you are a system administrator, you see information across domains. If you are a limited administrator with access rights to only one domain, you see information from only that domain.

Table 11-6 describes the **Home** page reports for Symantec Network Access Control.

Table 11-6 Symantec Network Access Control **Home** page summaries

Summary	Description
Failed Network Compliance Status	The Failed Network Compliance Status section provides a snapshot of the overall compliance in your network for the configured time period. It displays the clients that tried to connect to the network but cannot because they were out of compliance.
Compliance Status Distribution	Displays the clients that have failed the Host Integrity check that runs on their computer.

Table 11-6 Symantec Network Access Control **Home** page summaries *(continued)*

Summary	Description
Clients by Compliance Failure Summary	This summary displays the failure rate of the overall compliance requirement. It displays a bar chart that shows a count of the unique workstations by the type of control failure event. Examples of control failure event types are an antivirus, a firewall, or a VPN problem.
Compliance Failure Details	Provides a more detailed bar chart than the Clients by Compliance Failure Summary. For example, suppose the Clients by Compliance Failure Summary shows ten clients with an antivirus compliance failure. In contrast, this report shows the following details: ■ Four clients have no antivirus software currently in operation on them. ■ Two clients have no antivirus software installed. ■ Four clients have out-of-date antivirus definitions files.

If you have only Symantec Network Access Control installed, the **Home** page reports are not customizable, except for the time period covered by the reports and summaries. You can change the time period by using the Preferences link. The options are the past week and the past 24 hours.

Note: If you are a system administrator, you see information across domains. If you are a limited administrator with access rights to only one domain, you see information from only that one domain.

Using the Monitors Summary tab

The **Summary** tab on the **Monitors** tab displays concise, high-level summaries of important log data to give you an immediate picture of security status.

You can view the following summaries on the **Summary** tab:

- **Antivirus and TruScan Proactive Threat**
- **Network Threat Protection**
- **Compliance**

- **Site Status**

Table 11-7 lists the contents of the summary views.

Table 11-7 Summary views and their contents

Summary view	Contents
Antivirus and TruScan Proactive Threat	The **Antivirus and TruScan Proactive Threat** view contains the following information: ■ **TruScan Proactive Threat Scans** ■ **Risk Distribution** ■ **New Risks** ■ **Risk Distribution by Source** ■ **Risk Distribution by Attacker** ■ **Risk Distribution by Group** **Note:** New Risks are calculated from the last database sweep and for the time period that is configured on the **Home and Monitors** tab of **Preferences**. See "About Home and Monitors display options" on page 211. For example, suppose your **Preferences** time range is set to the past 24 hours. And suppose that your database is set to sweep every week on Sunday night and delete the risks that are more than three days old. If a particular virus infects a computer in your network on Monday, that is reported as a new risk. If another computer is infected with the same virus on Wednesday, that is not reflected in this count. If this same virus infects a computer in your network on the following Monday, it is reported here as newly infected. It is reported as new because it occurred during the last 24 hours and Sunday the database was swept of entries older than three days. The previous risk detections occurred more than three days ago, so they were deleted from the database.
Network Threat Protection	The **Network Threat Protection** view contains the following information: ■ **Top Targets Attacked by Group** ■ **Attack Event Types** ■ **Top Sources of Attack** ■ **Security Events by Severity**

Table 11-7 Summary views and their contents *(continued)*

Summary view	Contents
Compliance	The **Compliance** view contains the following information: ■ **Failed Network Compliance Status** ■ **Compliance Status Distribution** ■ **Clients by Compliance Failure Summary** ■ **Compliance Failure Details** **Note:** If you do not have Symantec Network Access Control installed, the **Compliance** view contains no data.
Site Status	The **Site Status** view contains the following information: ■ **Site Status** ■ **Top Error Generators By Server** ■ **Top Error Generators By Client** ■ **Replication Failures Over Time** ■ **Top Error Generators By Enforcer** **Note:** If you do not have Symantec Network Access Control installed, **Top Error Generators By Enforcer** contains no data.

If you have only Symantec Network Access Control installed, you should note the following information:

- The **Compliance** view that is described in Table 11-7 comprises your **Home** page.
- **Site Status** is the only view available on your **Summary** tab.

You can click any of the pie charts in the **Summary** tab view to see more details. For the **Top Targets Attacked by** summary under **Network Threat Protection**, use the list box to see the summary by groups, subnets, clients, or ports.

Note: If you have only Symantec Endpoint Protection installed, the charts in the **Compliance** summary view are empty. If you have only Symantec Network Access Control installed, the **Summary** tab contains only the **Site Status** view. You can view the **Compliance** summary information on the **Home** page.

To change the summary type

1. In the main window, click **Monitors**.
2. At the top of the **Summary** tab, in the **Summary type** list box, select the type of view that you want to see.

Configuring reporting preferences

You can configure the following reporting preferences:

- The **Home** and **Monitors** pages display options
- The **Security Status** thresholds
- The display options that are used for the logs and the reports, as well as legacy log file uploading

For information about the preference options that you can set, you can click **Help** on each tab in the **Preferences** dialog box.

To configure reporting preferences

1. From the console, on the **Home** page, click **Preferences**.
2. Click one of the following tabs, depending on the type of preferences that you want to set:
   - **Home and Monitors**
     See "About Home and Monitors display options" on page 211.
   - **Security Status**
     See "Configuring security status thresholds" on page 212.
   - **Logs and Reports**
     See "Configuring logs and reports preferences" on page 213.
3. Set the values for the options that you want to change.
4. Click **OK**.

About Home and Monitors display options

You can set the following preferences for the Home page and the Summary View tab of the Monitors page:

- The unit of time that is used for the reports on the Home page and on the Summary View tab on the Monitors page
- The rate at which the Home page and the Summary View tab on the Monitors page automatically refresh

- The extent of the notifications that are included in the unacknowledged notifications count on the Home page
- The content of the Action Summary on the Home page

By default, you see information for the past 24 hours, but you can change it to the past week if desired.

You can also configure the rate at which the Home page and the Summary View tab on the Monitors page automatically refresh. Valid values range from never to every 5 minutes.

Note: To configure the rate at which individual logs refresh, you can display the log you want to see. Then, you can select the rate that you want from the Auto-Refresh list box on that log's view.

If you are a system administrator, you can configure the Home page count to include only the notifications that you created but have not acknowledged. By default, system administrators see the total number of unacknowledged notifications, regardless of who created the notifications. If you are a limited administrator, the unacknowledged notifications count always consists solely of the notifications that you yourself created but have not acknowledged.

You can configure the Action Summary on the Home page to display by detection count on computers or by the number of computers.

See "About the Symantec Endpoint Protection Home page" on page 198.

For descriptions of these display options, see the context-sensitive help for the Home and Monitors tab. You can access the context-sensitive help from the Preferences link on the Home page.

See "Configuring reporting preferences" on page 211.

Configuring security status thresholds

The security status thresholds that you set determine when the Security Status message on the Home page of the Symantec Endpoint Protection Manager console is considered Poor. Thresholds are expressed as a percentage and reflect when your network is considered to be out of compliance with your security policies. For example, you can set the percentage of computers with out-of-date virus definitions that triggers a poor security status. You can also set how many days old the definitions need to be to qualify as out of date. Symantec Endpoint Protection determines what is current when it calculates whether signatures or definitions are out of date as follows. Its standard is the most current virus

definitions and IPS signature dates that are available on the management server on which the console runs.

Note: If you have only Symantec Network Access Control installed, you do not have a Security Status tab for configuring security thresholds.

For descriptions of these display options, see the context-sensitive help for the Security Status tab. You can access the context-sensitive help from the Preferences link on the Home page.

See "Configuring reporting preferences" on page 211.

To configure security status thresholds

1. From the console, on the Home page, click **Preferences**.
2. On the Security Status tab, check the items that you want to include in the criteria that determine the overall Home page security status.
3. For each item, type the number that you want to trigger a security status of Attention Needed.
4. Click **OK**.

Configuring logs and reports preferences

You can set preferences in the following areas for logs and reports:

- The date format and the date separator that are used for date display
- The number of rows, the time zone, and the IP address format that are used for table display
- The filter display in reports and notifications
- The availability of log data from the computers in the network that run Symantec Antivirus 10.x software

For descriptions of these display options, see the context-sensitive help for the Logs and Reports tab. You can access the context-sensitive help from the Preferences link on the Home page.

Note: The date display format that you set here does not apply to the virus definitions dates and the versions that display in table columns. These items always use the format Y-M-D.

See "Configuring reporting preferences" on page 211.

Eliminating viruses and security risks

Eliminating virus infections and security risks is a task you can perform either every day or as needed, depending on your network's security status. First, you identify and locate the risks, then decide how to handle them. After you remediate problems, you can update the Computer Status log to show that you have responded to the risks.

For more information about virus troubleshooting, see the following document in the Symantec Knowledge Base: *The 5 Steps of Virus Troubleshooting* (document ID 2007011014341948).

Table 11-8 Steps to eliminate viruses and security risks

Step	Description
Identify any infected client computers, or computers that are at risk	See "Identifying the infected and at risk computers" on page 215.
Determine why the computers are infected or at risk	You can check to make sure that all computers have Symantec Endpoint Protection installed and configured properly. You can run updates and scans to make sure that you review the most current list of infections and risks. See "Updating definitions and rescanning" on page 218.

Table 11-8 Steps to eliminate viruses and security risks *(continued)*

Step	Description
Remediate the infection or the risk	Remediation depends on the type of infection or risk. You can remediate in any of the following ways: ■ Review the actions that are associated with scans and rescan the infected or at risk computers. See "Changing an action and rescanning the identified computers" on page 216. See "Restarting the computers that need a restart to finish remediation" on page 217. ■ Investigate and clean remaining risks. See "About investigating and cleaning the remaining risks" on page 217. ■ Eliminate any suspicious events (Windows clients only). See "How to eliminate a suspicious event" on page 217.

Identifying the infected and at risk computers

The first task is to identify the computers that are infected and at risk.

See "Eliminating viruses and security risks" on page 214.

To identify infected computers

1 In the console, click **Home** and look at the Action Summary.

If you are a system administrator, you see counts of the number of Newly Infected and Still infected computers in your site. If you are a domain administrator, you see counts of the number of Newly Infected and Still infected computers in your domain. Still Infected is a subset of Newly Infected, and the Still Infected count goes down as you eliminate the risks from your network. Computers are still infected if a subsequent scan would report them as infected. For example, Symantec Endpoint Protection might have been able to clean a risk only partially from a computer and thus Auto-Protect still detects the risk.

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

3 In the Report type list box, click **Risk**.

4 In the Select a report list box, click **Infected and At Risk Computers**.

5 Click **Create Report** and note the lists of the infected and at risk computers that appear.

Changing an action and rescanning the identified computers

The next step in the remediation of the risks in your network is to identify why the computers are still infected or at risk. Check the action that was taken for each risk on the infected and at risk computers. It may be that the action that was configured and taken was Left Alone. If the action was Left Alone, you should either clean the risk from the computer, remove the computer from the network, or accept the risk. You may want to edit the Antivirus and Antispyware Policy that is applied to the group that this computer is in. You may want to configure a different action for this category of risks, or for this specific risk.

To identify the actions that need to be changed and rescan the identified computers

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

2 In the Logs tab, select the Risk log, and then click **View Log**.

From the Risk log event column, you can see what happened and the action that was taken. From the Risk Name column, you can see the names of the risks that are still active. From the Domain Group User column you can see which group the computer is a member of.

If a client is at risk because a scan took the action Left Alone, you may need to change the Antivirus and Antispyware Policy for the group. From the Computer column, you can see the names of the computers that still have active risks on them.

See "Configuring actions for known virus and security risk detections on Windows clients" on page 417.

If your policy is configured to use Push mode, it is pushed out to the clients in the group at the next heartbeat.

See "Configuring push mode or pull mode to update client policies and content" on page 109.

3 Click **Back**.

4 In the Logs tab, select the Computer Status log, and then click **View Log**.

5 If you changed an action and pushed out a new policy, select the computers that need to be rescanned with the new settings.

6 From the Command list box, select Scan, and then click **Start** to rescan the computers.

You can monitor the status of the Scan command from the Command Status tab.

Restarting the computers that need a restart to finish remediation

Computers may still be at risk or infected because they need to be restarted to finish the remediation of a virus or security risk.

See "Eliminating viruses and security risks" on page 214.

To restart computers to finish remediation

1 In the Risk log, check the Restart Required column.

It may be that a risk was partially cleaned from some computers, but the computers still require a restart to finish the remediation.

2 Select the computers in the list that require a restart.

3 In the Command list box, select Restart Computers, and then click **Start**.

You can monitor the status of the Restart Computers command from the Command Status tab.

About investigating and cleaning the remaining risks

If any risks remain, you may need to investigate them further.

From the scan results dialog box, you can click the link to Symantec Security Response for the detected risk. The scan results also tell you what processes, files, or registry keys are involved in the risk detection.

You may be able to create a custom Application Control policy to block an offending application.

See "Creating an Application and Device Control Policy" on page 545.

Or, you may need to disconnect the computer from the network and delete files and Windows registry keys and stop processes manually.

How to eliminate a suspicious event

A suspicious security risk indicates that a TruScan proactive threat scan has detected something that you should investigate. It may or may not be harmless. If you determine that this risk is harmless, you can use the Centralized Exceptions

Policy to exclude it from detection in the future. If the proactive threat scans cannot remediate a risk or if you have configured it to leave a risk alone, you may need to eliminate those risks.

If you configured TruScan proactive threat scans to log, and you investigate and determine that a risk is harmful, you can remediate it with the Centralized Exceptions Policy. Configure the Centralized Exceptions Policy to terminate or quarantine the risk instead of logging it.

See "Configuring a centralized exception for TruScan proactive threat scans" on page 584.

If Symantec Endpoint Protection detected this risk by using the default TruScan proactive threat scan settings, then Symantec Endpoint Protection cannot remediate this risk. If you determine that this risk is harmful, you should remove the risk manually. After you have removed the risk, you can delete that entry from the Risk log.

Updating definitions and rescanning

Some computers can still be at risk because their definitions are out-of-date.

See "Managing content for clients" on page 132.

To update definitions and rescan

1. For the remaining computers in the view, check the Definitions Date column. If some computers have virus definitions that are out of date, select those computers.
2. In the Command list box, select Update Content and Scan, and then click **Start**.

   You can monitor the status of the Update Content and Scan command from the Command Status tab.
3. Click **Home** and look at the numbers in the Action Summary Still Infected and Newly Infected rows.

   If the counts are zero, you have eliminated the risks. If the counts are not zero, you should investigate the remaining risks.

Finding the clients that are offline

You can check to see which computers are offline in your network in several ways.

For example, you can perform the following checks:

- Run the Computer Status quick report Computers Not Checked into Server to see online status.

- Configure and run a custom version of this report to look at the computers in a particular group or site.
- View the Computer Status log, which contains the computer's IP address, and time of last check-in.

See "About the reports you can run" on page 221.

A client may be offline for a number of reasons. You can identify the computers that are offline and remediate these problems in a number of ways.

If you have Symantec Network Access Control installed, you can use the Compliance filter options to customize the Computers Not Checked into Server quick report. You can then use this report to look at the specific reasons that computers are not on the network. You can then eliminate the problems that you see.

Among the compliance reasons you can filter on are the following reasons:

- The computer's antivirus version is out-of-date.
- The computer's antivirus software is not running.
- A script failed.
- The computer's location has changed.

To find the clients that are offline

1. In the console, click **Monitors**.
2. On the Logs tab, from the Log type list box, click **Computer Status**.
3. Click **Advanced Settings**.
4. In the Online status list box, click **Offline**.
5. Click **View Log**.

   By default, a list of the computers that have been offline for the past 24 hours appears. The list includes each computer's name, IP address, and the last time that it checked in with its server. You can adjust the time range to display offline computers for any time range you want to see.

Chapter 12

Viewing and configuring reports

This chapter includes the following topics:

About the reports you can run

You can view predefined quick reports, and you can generate custom reports that are based on the filter settings you select. You can also save filter configurations

to generate the same custom reports in the future and delete them when they are no longer needed.

Also, you can schedule reports to run at regular intervals. The reports are emailed to specified recipients.

Table 12-1 describes the types of reports that are available.

Table 12-1 Report types

Report type	Description
Audit	Displays information about the policies that clients and locations use currently. It includes information about policy modification activities, such as the event times and types, policy modifications, domains, sites, administrators, and descriptions. See "About the information in the Audit report and log " on page 224.
Application and Device Control	Displays information about events where some type of behavior was blocked. These reports include information about application security alerts, blocked targets, and blocked devices. Blocked targets can be Windows registry keys, dlls, files, and processes. See "About the information in the Application Control and Device Control reports and logs" on page 225.
Compliance	Displays information about the compliance status of your network. These reports include information about Enforcer servers, Enforcer clients, Enforcer traffic, and host compliance. See " About the information in the Compliance reports and logs " on page 226.
Computer Status	Displays information about the operational status of the computers in your network, such as which computers have security features turned off. These reports include information about versions, the clients that have not checked in to the server, client inventory, and online status. See "About the information in the Computer Status reports and log" on page 227.

Table 12-1 Report types *(continued)*

Report type	Description
Network Threat Protection	Displays information about intrusion prevention, attacks on the firewall, and about firewall traffic and packets. The Network Threat Protection reports allow you to track a computer's activity and its interaction with other computers and networks. They record information about the traffic that tries to enter or exit the computers through their network connections. See "About the information in the Network Threat Protection reports and logs" on page 231.
Risk	Displays information about risk events on your management servers and their clients. It includes information about TruScan proactive threat scans. See "About the information in the Risk reports and log" on page 235. See "About the information in the TruScan proactive threat scan reports and logs" on page 234.
Scan	Displays information about antivirus and antispyware scan activity. See "About the information in the Scan reports and log" on page 238.
System	Displays information about event times, event types, sites, domains, servers, and severity levels. See "About the information in the System reports and logs" on page 239.

You can configure basic settings and advanced settings for all reports to refine the data you want to view. You can modify the predefined reports and save your configuration. You can also save your custom filter with a name to run the same custom report at a later time. You can also delete your customized configurations if you don't need them anymore. The active filter settings are listed in the report if you have configured the log and report preferences setting to include the filters in reports.

If you have multiple domains in your network, many reports allow you to view data for all domains, one site, or a few sites. The default for all quick reports is to show all domains, groups, servers, and so on, as appropriate for the report you select to create.

See "About quick reports" on page 246.

See "Creating quick reports" on page 250.

Note: Some predefined reports contain information that is obtained from Symantec Network Access Control. If you have not purchased that product, but you run one of that product's reports, the report is empty.

Note: If you have only Symantec Network Access Control installed, a significant number of reports are empty. The **Application and Device Control**, **Network Threat Protection**, **Risk**, and **Scan** reports do not contain data. The **Compliance** and **Audit** reports do contain data, as do some of the **Computer Status** and **System** reports.

See "Configuring logs and reports preferences" on page 213.

When you create a report, the report appears in a separate window. You can save a copy of the report in Web archive format or you can print a copy of the report. The saved file or printed report provides a snapshot of the current data in your reporting database so that you can retain a historical record.

You can also create scheduled reports that are automatically generated based on a schedule that you configure. You set the report filters and the time to run the report. When the report is finished, it is emailed to one or more recipients.

A scheduled report always runs by default. You can change the settings for any scheduled report that has not yet run. You can also delete a single scheduled report or all of the scheduled reports.

See "About scheduled reports" on page 254.

See "Creating and deleting scheduled reports" on page 255.

About the information in the Audit report and log

The **Audit** log contains information about policy modification activities, such as the event times and types, policy modifications, domains, sites, administrators, and descriptions.

The default **Audit** quick report is called **Policies Used**. View the **Policies Used** report to monitor the policies in use in your network, by group. You can look at the **Audit** log when you want to see which administrator changed a particular policy and when.

See "About the reports you can run" on page 221.

About the information in the Application Control and Device Control reports and logs

Application and Device Control logs and reports include information about the **Application and Device Control** Policies and **Tamper Protection**. The logs contain information about the following types of events:

- Access to a computer entity was blocked
- A device was kept off the network

Files, Windows registry keys, and processes are examples of computer entities.

Table 12-2 describes some typical uses for the kind of information that you can get from Application Control and Device Control reports and logs.

Table 12-2 Application Control and Device Control reports and logs summary

Report or log	Typical uses
Top Groups with Most Alerted Application Control Logs report	Use this report to check which groups are most at risk in your network.
Top Targets Blocked report	Use this report to check which files, processes, and other entities are used most frequently in attacks against your network.
Top Devices Blocked report	This report consists of a pie chart with a relative bar that shows the devices most frequently blocked from access to your network.
Application Control log	Use this log to see information about the following entities: ■ The actions that were taken in response to events ■ The processes that were involved in the events ■ The rule names that were applied from a policy when an application's access was blocked You can take the action to add a file to the **Centralized Exceptions** Policy as a result of an event in the **Application Control** log. See "Creating centralized exceptions from log events" on page 587.
Device Control log	Use this log when you need to see **Device Control** details, such as the exact time that **Device Control** enabled or disabled devices. This log also displays information such as the name of the computer, its location, the user who was logged on, and the operating system involved.

See "About the reports you can run" on page 221.

About the information in the Compliance reports and logs

The **Compliance** reports and logs contain information about the Enforcer server, clients, and traffic, and about host compliance. The information available includes items such as the time and the event type, the name of the Enforcer involved, the site, and the server.

Note: If you do not have Symantec Network Access Control installed, the **Compliance** logs and reports do not contain any data.

Table 12-3 describes some typical uses for the kind of information that you can get from **Compliance** reports and logs.

Table 12-3 Compliance reports and logs summary

Report or log	Typical uses
Network Compliance Status report	Use this report to look at overall compliance, to see if clients have failed Host Integrity checks or authentication, or have been disconnected.
Compliance Status report	Use this report to see the total number of clients that have either passed or failed a Host Integrity check in your network.
Clients by Compliance Failure Summary report	Use this report to see the general reasons for control failure events, such as antivirus, firewall, or VPN.
Compliance Failure Details report	Use this report to see a greater level of detail about the compliance failures. It shows the criteria and the rule that was involved in each failure. It includes the percentage of clients that have been deployed and the percentage that failed. For example, the **Compliance Failure Summary** can show ten client failures due to the antivirus software. In contrast, **Compliance Failure Details** shows the following information: ■ Four clients have no antivirus software currently in operation on them. ■ Two clients have no antivirus software installed. ■ Four clients have out-of-date antivirus definitions files.
Non-compliant Clients by Location report	This report consists of a table that shows the compliance failure events. These events display in groups that are based on their location. Information includes the unique computers that failed, and the percentage of total failures and location failures.

Table 12-3 Compliance reports and logs summary *(continued)*

Report or log	Typical uses
Enforcer Server log	Use this log to look at information about Enforcer compliance events, the name of the Enforcer involved, its site, and its server. Among other things, this log contains the following information: ■ Which Enforcers were unable to register with their servers ■ Which Enforcers have successfully received downloads of policies and the sylink.xml communication file ■ Whether or not the Enforcers' server has successfully received the Enforcers' logs
Enforcer Client log	Use this log to see which clients have passed or failed Host Integrity checks, were authenticated or rejected, or were disconnected from the network.
Enforcer Traffic log	Use this log to look at information about the traffic that moves through an Enforcer. The information available includes: ■ The direction of the traffic ■ The time when the traffic began and the time when the traffic ended ■ The protocol used ■ The source IP address and destination IP address that was used ■ The port that was used ■ The packet size (in bytes) ■ The attempted connections that were allowed or blocked This log applies only to Gateway Enforcers.
Host Compliance log	Use this log to look at specific information about particular compliance events. Such events include the reason, the user involved, and the name of the operating system that was involved.

See "About the reports you can run" on page 221.

About the information in the Computer Status reports and log

The Computer Status reports and log contains information about the real-time operational status of the computers in the network. Information available includes the computer name and IP address, last check-in time, definitions date, infected status, Auto-Protect status, server, group, domain, and user name. Filters for Computer Status reports have both standard configuration options and compliance-specific options.

Table 12-4 describes some typical uses for the kind of information that you can get from Computer Status reports and logs.

Table 12-4 Computer Status reports and log summary

Report or log	Typical uses
Virus Definitions Distribution report	Use this report to make sure that all the groups, domains, or servers in your network use up-to-date virus definitions files versions. This report displays the unique virus definitions file versions that are used throughout your network and the number of computers and percentage using each version. It consists of a pie chart, a table, and relative bars.
Computers Not Checked into Server report	Use this report to find the computers that have not checked in with a server and therefore might be lost or missing. The report displays the computer's IP address, the time of its last check in, and the user that was logged in at that time.
Symantec Endpoint Protection Product Versions report	Use this report to check the versions of Symantec Endpoint Protection software, virus definitions, IPS signatures, and proactive protection content in use in your network. Information includes the domain and server for each, as well as the number of computers and percentage of each. It consists of a pie chart and relative bars. With this information, you can pinpoint the computers that need an update.
Intrusion Prevention Signature Distribution report	Use this report to make sure that all the groups in your network use up-to-date intrusion prevention signatures. You can also see which domains or servers are out-of-date. It consists of a pie chart and relative bars.
Client Inventory report	Use this report to see the number and percentage of computers that fall into certain hardware and software categories. This report consists of the following charts with relative bars that display the total number of computers and percentage of each: ■ Operating System ■ Total Memory ■ Free Memory ■ Total Disk Space ■ Free Disk Space ■ Processor Type For example, from the Client Inventory report, you might see that 22% of your computers have less than 1 GB of free disk space.

Table 12-4 Computer Status reports and log summary *(continued)*

Report or log	Typical uses
Compliance Status Distribution report	Use this report, which consists of a pie chart with relative bars, to view compliance passes and failures by group or by subnet. It shows the number of computers and the percentage of computers that are in compliance. You may want to investigate if certain groups seem to have a lot more compliance problems than others.
Client Online Status report	Use this report to see which groups or subnets have the largest percentage of clients online. This report consists of pie charts with relative bars per group or per subnet. Online has the following meanings: ■ For the clients that are in push mode, online means that the clients are currently connected to the server. ■ For the clients that are in pull mode, online means that the clients have contacted the server within the last two client heartbeats. ■ For the clients in remote sites, online means that the clients were online at the time of the last replication. You may want to investigate why some groups or subnets currently experience more problems than others.
Clients With Latest Policy quick report **Distribution of Clients by Policy** scheduled report	Use this report to see the number of computers and percentage that have the latest policy applied. This report consists of pie charts with relative bars per group or subnet.
Client Count by Group report	Use this report to see the total number of clients and users, by group. If you use multiple domains, this information appears by domain.
Security Status Summary report	Use this report to quickly see the total number of computers that have the following problems: ■ Auto-Protect is disabled ■ The Antivirus engine is turned off ■ Tamper Protection is turned off ■ The computer needs to be restarted ■ The computer failed a host integrity check ■ Network Threat Protection is turned off These computers may continue to be at risk unless you intervene.

Table 12-4 Computer Status reports and log summary *(continued)*

Report or log	Typical uses
Protection Content Versions report	Use this report to check the versions of Proactive Protection content that are used throughout your network in a single report. One pie chart is displayed for each type of protection. The following content types are available: ■ Decomposer versions ■ Eraser Engine versions ■ TruScan Proactive Threat Scan Content versions ■ TruScan Proactive Threat Scan Engine versions ■ Commercial Application List versions ■ Proactive Content Handler Engine versions ■ Permitted Applications List versions ■ The new content types that Symantec Security Response has added
Client Migration report	Use this report to see the migration status of clients by domain, group, and server. You can quickly identify clients where migration has succeeded, failed, or has not yet started.
Client Software Rollout (Snapshots) report This report is available as a scheduled report only.	Use this report to track the progression of client package deployments. The snapshot information lets you see how quickly the rollout progresses, as well as how many clients are still not fully deployed.
Clients Online/Offline Over Time (Snapshots) report This report is available as a scheduled report only.	Use this report to pinpoint the clients that don't connect to the network frequently enough.
Clients With Latest Policy Over Time (Snapshots) report This report is available as a scheduled report only.	Use this report to pinpoint the clients that don't get policy updates frequently enough.
Non-compliant Clients Over Time (Snapshots) report This report is available as a scheduled report only.	Use this report to pinpoint the clients that frequently fail host integrity checks.

Table 12-4 Computer Status reports and log summary *(continued)*

Report or log	Typical uses
Virus Definitions Rollout (Snapshots) report This report is available as a scheduled report only.	Use this report to see the list of the virus definitions package versions that have been rolled out to clients.
Computer Status log	Check the Computer Status log if you need more details about any of the areas that the reports cover.

See "About the reports you can run" on page 221.

About the information in the Network Threat Protection reports and logs

Network Threat Protection reports and logs let you track a computer's activity and its interaction with other computers and networks. They record information about the traffic that tries to enter or exit the computers through their network connections.

Network Threat Protection logs contain details about attacks on the firewall, such as the following information:

- Denial-of-service attacks
- Port scans
- Changes that were made to executable files

Network Threat Protection logs collect information about intrusion prevention. They also contain information about the connections that were made through the firewall (traffic), the Windows registry keys, files, and DLLs that are accessed. They contain information about the data packets that pass through the computers. The operational changes that were made to computers are also logged in these logs. This information may include when services start and stop or when someone configures software. Among the other types of information that may be available are items such as the time and the event type and the action taken. It can also include the direction, host name, IP address, and the protocol that was used for the traffic involved. If it applies to the event, the information can also include the severity level.

Table 12-5 describes some typical uses for the kind of information that you can get from **Network Threat Protection** reports and logs.

Table 12-5 Network Threat Protection reports and logs summary

Report or log	Typical uses
Top Targets Attacked report	Use this report to identify which groups, subnets, computers, or ports are attacked most frequently. It includes information such as the number and percentage of attacks, the attack type and severity, and the distribution of attacks. You may want to take some action based on this report. For example, you might find that the clients that attach through a VPN are attacked much more frequently. You might want to group those computers so that you can apply a more stringent security policy.
Top Sources of Attack report	Use this report to identify which hosts attack your network most frequently. This report consists of a pie chart with relative bars that shows the top hosts that initiated attacks against your network. It includes information such as the number and percentage of attacks, the attack type and severity, and the distribution of attacks.
Top Types of Attack report	Use this report to identify the types of attack that are directed at your network most frequently. The possible types of attack that you can monitor include port scans, denial-of-service attacks, and MAC spoofing. This report consists of a pie chart with associated relative bars. It includes information such as the number and percentage of events. It also includes the group and severity, as well as the event type and number by group.
Top Blocked Applications report **Blocked Applications Over Time** report	Use these reports together to identify the applications that are used most frequently to attack your network. You can also see whether or not the applications being used for attacks have changed over time. The **Top Blocked Applications** report consists of a pie chart with relative bars that show the top applications that were prevented from accessing your network. It includes information such as the number and percentage of attacks, the group and severity, and the distribution of attacks by group. The **Blocked Applications Over Time** report consists of a line chart and table. It displays the total number of applications that were prevented from accessing your network over a time period that you select. It includes the event time, the number of attacks, and the percentage. You can display the information for all computers, or by group, IP address, operating system, or user.

Table 12-5 Network Threat Protection reports and logs summary *(continued)*

Report or log	Typical uses
Attacks over Time report	Use this report to identify the groups, IP addresses, operating systems, and users that are attacked most frequently in your network. Use it to also identify the most frequent type of attack that occurs. This report consists of one or more line charts that display attacks during the selected time period. For example, if the time range is the last month, the report displays the total number of attacks per day for the past month. It includes the number and percentage of attacks. You can view attacks for all computers, or by the top operating systems, users, IP addresses, groups, or attack types.
Security Events by Severity report	Use this report to see a summary of the severity of security events in your network. This report consists of a pie chart that displays the total number and percentage of security events in your network, ranked according to their severity.
Top Traffic Notifications report **Traffic Notifications Over Time** report	Use these reports to show the number of attacks that violated the firewall rules that you configured to notify you about violations. Use them to see which groups are most at risk of attack through the firewall. The **Top Traffic Notifications** report consists of a pie chart with relative bars that lists the group or subnet, and the number and percentage of notifications. It shows the number of notifications that were based on firewall rule violations that you configured as important to be notified about. The rules that are counted are those where you checked the **Send Email Alert** option in the **Logging** column of the **Firewall Policy Rules** list. You can view information for all, for the **Traffic** log, or for the **Packet** log, grouped by top groups or subnets. The **Traffic Notifications Over Time** report consists of a line chart. It shows the number of notifications that were based on firewall rule violations over time. The rules that are counted are those where you checked the **Send Email Alert** option in the **Logging** column of the **Firewall Policy Rules** list. You can display the information in this report for all computers, or by group, IP address, operating system, or user.

Table 12-5 Network Threat Protection reports and logs summary *(continued)*

Report or log	Typical uses
Full Report report	Use this report to see the information that appears in all the Network Threat Protection quick reports in one place. This report gives you the following Network Threat Protection information in a single report: ■ Top Types of Attack ■ Top Targets Attacked by Group ■ Top Targets Attacked by Subnet ■ Top Targets Attacked by Client ■ Top Sources of Attack ■ Top Traffic Notifications by Group (Traffic) ■ Top Traffic Notifications by Group (Packets) ■ Top Traffic Notifications by Subnet (Traffic) ■ Top Traffic Notifications by Subnet (Packets)
Attacks log	Use this log if you need more detailed information about a specific attack that occurred.
Traffic log	Use this log if you need more information about a specific traffic event or type of traffic that passes through your firewall.
Packets log	Use this log if you need more information about a specific packet. You may want to look at packets to more thoroughly investigate a security event that was listed in a report.

See "About the reports you can run" on page 221.

About the information in the TruScan proactive threat scan reports and logs

Table 12-6 describes some typical uses for the kind of information that you can get from **TruScan proactive threat scan** reports and log.

Table 12-6 **TruScan proactive threat scan** reports and logs summary

Report or log	Typical uses
TruScan Proactive Threat Scan Detection Results report (located under Risk reports) **TruScan Proactive Threat Detection Over Time** report (located under Risk reports)	Use the **TruScan Proactive Threat Scan Detection Results** report to see the following information: ■ A list of the applications that are labeled as risks that you have added to your exceptions as acceptable in your network ■ A list of the applications that have been detected that are confirmed risks ■ A list of the applications that have been detected but whose status as a risk is still unconfirmed Use the **TruScan Proactive Threat Detection Over Time** report to see if the threats detected by TruScan proactive threat scans have changed over time.
TruScan Proactive Threat Distribution report (located under Risk reports)	Use this report for the following reasons: ■ To see which applications from the Commercial Applications List and Forced Detections list are detected most frequently ■ To see what action was taken in response to the detection ■ To determine if particular computers in your network are attacked more frequently by this vector ■ To see details about the application that attacked
TruScan Proactive Threat Scan log	Use this log if you need more information about specific proactive threat detection events. This information can be something like the name of the user that was logged on when the detection occurred. You can also use commands from this log to add legitimate entities such as files, folders, extensions, and processes to the **Centralized Exceptions** Policy. After they are added to the list, if a legitimate activity is detected as a risk, the entity is not acted upon.

See "About the reports you can run" on page 221.

About the information in the Risk reports and log

The **Risk** reports and log include information about risk events on your management servers and their clients. Also, **TruScan proactive threat scan** activity is reported in **Risk** reports.

See "About the information in the TruScan proactive threat scan reports and logs" on page 234.

Table 12-7 describes some typical uses for the kind of information that you can get from Risk reports and log.

Table 12-7 Risk reports and log summary

Log and report types	Typical uses
Infected and At Risk Computers report	Use this report to quickly identify the computers that need your attention because they are infected with a virus or a security risk. This report consists of two tables. One table lists computers that have a virus infection. The other table lists the computers that have a security risk that has not yet been remediated.
Detection Action Summary report	Use this report to identify the actions that were taken when risks were detected. This information also appears on the Symantec Endpoint Protection **Home** page. This report consists of a table that shows a count of all the possible actions that were taken when risks were detected. The possible actions are Cleaned, Suspicious, Blocked, Quarantined, Deleted, Newly Infected, and Still Infected. This information also appears on the Symantec Endpoint Protection Home page.
Risk Detections Count report	Use this report to identify the domains, groups, or particular computers that have the largest number of risk detections. You can then investigate why some entities seem to be at greater risk than others in your network. This report consists of a pie chart, a risk table, and an associated relative bar. It shows the total number of risk detections by domain, server, or computer. If you have legacy Symantec AntiVirus clients, the report uses the server group rather than the domain.
New Risks Detected in the Network report	Use this report to identify and track the impact of new risks on your network. This report includes a table and a distribution pie chart. For each new risk, the table provides the following information: ■ Risk name ■ Risk category or type ■ First discovered date ■ First occurrence in the organization ■ Scan type that first detected it ■ Domain where it was discovered (server group on legacy computers) ■ Server where it was discovered (parent server on legacy computers) ■ Group where it was discovered (parent server on legacy computers) ■ The computer where it was discovered and the name of the user that was logged on at the time The pie chart shows new risk distribution by the target selection type: domain (server group on legacy computers), group, server (parent server on legacy computers), computer, or user name.

Table 12-7 Risk reports and log summary *(continued)*

Log and report types	Typical uses
Top Risk Detections Correlation report	Use this report to look for correlations between risks and computers, users, domains, and servers. This report consists of a three-dimensional bar graph that correlates virus and security risk detections by using two variables. You can select from computer, user name, domain, group, server, or risk name for the x and y axis variables. This report shows the top five instances for each axis variable. If you selected computer as one of the variables and there are fewer than five infected computers, non-infected computers may appear in the graph. **Note:** For computers running legacy versions of Symantec AntiVirus, the server group and parent server are used instead of domain and server.
Risk Distribution Summary report **Risk Distribution Over Time** report	Use these reports to track the distribution of risks. You can also use it to pinpoint particular risks, domains, groups, servers, computers, and the users that seem to have more problems than others. You can use **Risk Distribution Over Time** to see how these risks change over time. The **Risk Distribution Summary** report includes a pie chart and an associated bar graph that displays a relative percentage for each unique item from the chosen target type. For example, if the chosen target is risk name, the pie chart displays slices for each unique risk. A bar is shown for each risk name and the details include the number of detections and its percentage of the total detections. Targets include the risk name, domain, group, server, computer, user name, source, risk type, or risk severity. For computers running legacy versions of Symantec AntiVirus, the server group and parent server are used instead of domain and server. The **Risk Distribution Over Time** report consists of a table that displays the number of virus and security risk detections per unit of time and a relative bar.
Action Summary for Top Risks report	Use this report to review the actions that were taken on the risks that Symantec Endpoint Protection has detected in your network. This report lists the top risks that have been found in your network. For each, it displays action summary bars that show the percentage of each action that was taken when a risk was detected. Actions include quarantined, cleaned, deleted, and so on. This report also shows the percentage of time that each particular action was the first configured action, the second configured action, neither, or unknown.

Table 12-7 Risk reports and log summary *(continued)*

Log and report types	Typical uses
Number of Notifications report **Number of Notifications Over Time** report	Use these reports to refine how you create and configure notifications in your network. The **Number of Notifications** report consists of a pie chart with an associated relative bar. The charts show the number of notifications that were triggered by the firewall rule violations that you have configured as important to be notified about. It includes the type of notifications and the number of each. See "Configuring email messages for traffic events" on page 513. The **Number of Notifications Over Time** report consists of a line chart that displays the number of notifications in the network for the time period selected. It also contains a table that lists the number of notifications and percentage over time. You can filter the data to display by the type of notification, acknowledgment status, creator, and notification name.
Weekly Outbreaks report	Use this report to track risk outbreaks week by week. This report displays the number of virus and security risk detections and a relative bar per week for each for the specified time range. A range of one day displays the past week.
Comprehensive Risk Report report	Use this report to see all of the distribution reports and the new risks report information at one time. By default, this report includes all of the distribution reports and the new risks report. However, you can configure it to include only certain of the reports. This report includes the information for all domains.
Risk log	Use this log if you need more specific information about any of the areas in the Risk reports. For example, you can use the Risk log to see details about the risks that were detected on the computers where risks are often found. You can also use the Risk log to see details about security risks of a particular severity that have affected your network.

See "About the reports you can run" on page 221.

About the information in the Scan reports and log

The **Scan** reports and log contain information about antivirus and antispyware scan activity.

Table 12-8 describes some typical uses for the kind of information that you can get from Scan quick reports and log.

Table 12-8 Scan reports and logs summary

Report or log	Typical uses
Scan Statistics Histogram report	Group by scan time when you use this report to see a histogram of how long it takes for scheduled scans to complete on clients. You might want to change the time the scan is scheduled for based on this information. You can filter this report based on the number of files that were scanned. These results can help you to see if any users restrict the scans to a small number of files on their computers. You can select how you want the information in the scan report to be distributed. You can select one of the following methods: ■ By the scan time (in seconds) ■ By the number of risks detected ■ By the number of files with detections ■ By the number of files that are scanned ■ By the number of files that are omitted from scans You can also configure the bin width and how many bins are used in the histogram. The bin width is the data interval that is used for the group by selection. The number of bins specifies how many times the data interval is repeated in the histogram. The information that displays includes the number of entries and the minimum and the maximum values, as well as the average and the standard deviation. You might want to change the report values to maximize the information that is generated in the report's histogram. For example, you might want to consider the size of your network and the amount of information that you view.
Computers by Last Scan Time report	Use this report to identify the computers that have not run a scan recently. You can configure it to look for the last day or the last week or a custom time period that you want to check.
Computers Not Scanned report	Use this report to get a list of the computers that have not been scanned for a specific time period. This report also tells you the computers' IP addresses by specific domains or by groups. These computers may be at risk.
Scan log	You can sort this log by scan duration to identify the computers that take the longest time to scan in your network. Based on this information, you can customize scheduled scans for these computers if needed.

See "About the reports you can run" on page 221.

About the information in the System reports and logs

The System reports and logs contain information that is useful for troubleshooting client problems.

Table 12-9 describes some typical uses for the kind of information that you can get from System quick reports and log.

Table 12-9 System reports and log summary

Report or log	Typical uses
Top Clients That Generate Errors report	Use this report to see which clients generate the largest number of errors and warnings. You may want to look at the location and type of users on these clients to see why they experience more problems than others. You can then go to the System log for details.
Top Servers That Generate Errors report	Use this report to see which servers generate the largest number of errors and warnings. You may want to look at these servers to see why they experience more problems than is typical for your network.
Top Enforcers That Generate Errors report	Use this report to see which Enforcers generate the largest number of errors and warnings. You may want to look at these Enforcers to see why they experience more problems than is typical for your network.
Database Replication Failures Over Time report	Use this report to see which servers or sites experience the most problems with database replication. It also tells you why the replications fail so that you can remediate the problems.

Table 12-9 System reports and log summary *(continued)*

Report or log	Typical uses
Site Status report	Use this report to see how your server handles its client load. Based on the information that is in this report, you may want to adjust the load. This report displays the current status and throughput of all servers in your local site. It also shows information about client installation, client online status, and client log volume for your local site. The data this report draws from is updated every ten seconds, but you need to rerun the report to see updated data. **Note:** If you have multiple sites, this report shows the total installed and online clients for your local site, not all your sites. If you have site or domain restrictions as an administrator, you only see the information that you are allowed to see. The health status of a server is classified as follows: ■ Good: The server is up and works normally ■ Poor: The server is low on memory or disk space, or has a large number of client request failures. ■ Critical: The server is down For each server, this report contains the status, health status and reason, CPU and memory usage, and free disk space. It also contains server throughput information, such as policies downloaded, and site throughput sampled from the last heartbeat. It includes the following site throughput information: ■ Total clients installed and online ■ Policies downloaded per second ■ Intrusion Prevention signatures downloaded per second ■ Learned applications per second ■ Enforcer system logs, traffic logs, and packet logs per second ■ Client information updates per second ■ Client security logs, system logs, traffic logs, and packet logs received per second ■ Application and device control logs received per second Online has the following meanings in this report: ■ For the clients that are in push mode, online means that the clients are currently connected to the server. ■ For the clients that are in pull mode, online means that the clients have contacted the server within the last two client heartbeats. ■ For the clients in remote sites, online means that the clients were online at the time of the last replication.

Table 12-9 System reports and log summary *(continued)*

Report or log	Typical uses
Administrative log	Use this log to look at administrative-related items like the following activities: ■ Logons and logoffs ■ Policy changes ■ Password changes ■ When certificates are matched ■ Replication events ■ Log-related events This log may be useful for troubleshooting client problems such as missing certificates, policies, or imports. You can look separately at events as they relate to domains, groups, users, computers, imports, packages, replications, and other events.
Client-Server Activity log	Use this log to look at all the client activity that takes place for a specific server. For example, you can use this log to look at the following items: ■ Successful and unsuccessful policy downloads ■ Client connections to the server ■ Server registrations
Server Activity log	Among other things, use this log for the following reasons: ■ To locate and troubleshoot replication problems ■ To locate and troubleshoot backup problems ■ To locate and troubleshoot Radius Server problems ■ To look at all server events of a particular severity level
Client Activity log	Among other things, you can use this log to monitor the following client-related activities: ■ Which clients have been blocked from accessing the network ■ Which clients need to be restarted ■ Which clients had successful or unsuccessful installations ■ Which clients had service initiation and termination problems ■ Which clients had rules import problems ■ Which clients had problems downloading policies ■ Which clients had failed connections to the server ■ The status of the client as a group update provider (GUP)

Table 12-9 System reports and log summary *(continued)*

Report or log	Typical uses
Enforcer Activity log	Use this log to monitor problems with the Enforcers. In this log, you can view management events, Enforcer events, enable events, and policy events. You can filter them by their severity level. For example, you can use this log to troubleshoot the following types of problems: ■ Enforcer connectivity ■ The importation and application of policies and configurations ■ Enforcer starts, stops, and pauses

Note: If you do not have Symantec Network Access Control installed, the **Enforcer Activity** log and the entries in other logs that apply to Enforcers are empty.

See "About the reports you can run" on page 221.

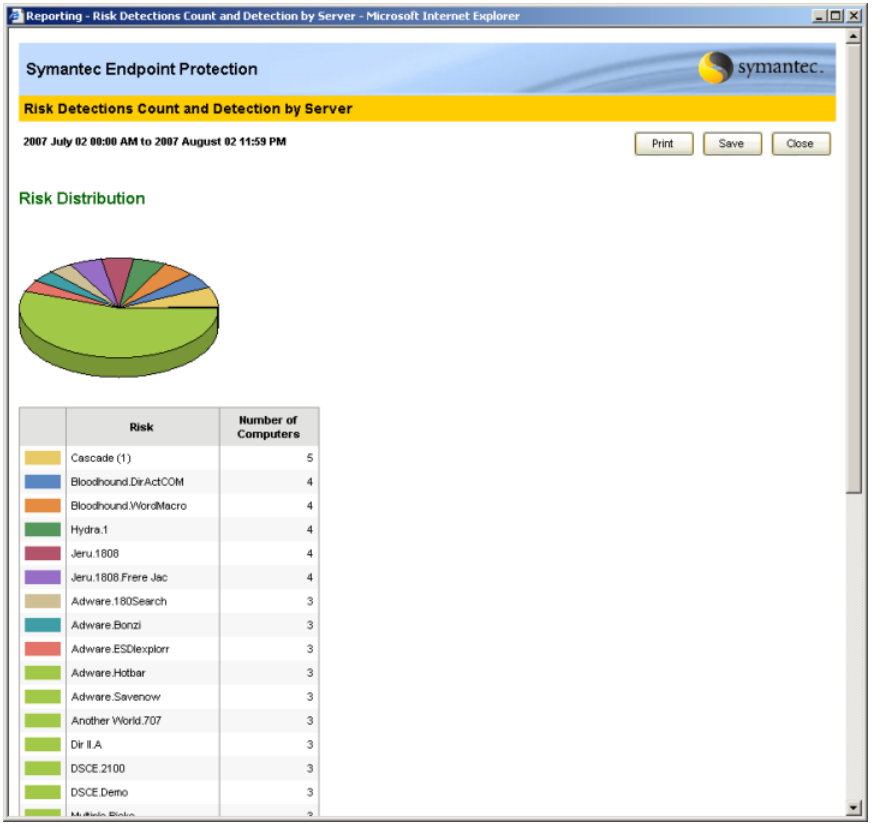
About viewing reports

Use the Reports page to run, view, and print reports, and to schedule reports to run on a regular basis.

The optimal display resolution for reporting functions is 1024 x 768 or higher. However, you can view the reporting functions with a screen resolution as low as 800 x 600 by using the scroll bars.

Figure 12-1 shows one of the risk reports that you can run.

Figure 12-1 Example of a risk report



About viewing line charts in reports

Line charts show progression over time. The units that are displayed on the x-axis depend on the time range you select.

Table 12-10 shows the x-axis unit that is used for each time range you can select for line charts.

Table 12-10 X-axis units for corresponding time range selected

Time range	X-axis unit
Past 24 Hours	hour

Table 12-10 X-axis units for corresponding time range selected *(continued)*

Time range	X-axis unit
Past Week Past Month Current Month Past 3 Months	day
Past Year	month
Time range	one day (any 24 hours) is by hour greater than 1 day but less than or equal to 7 days is by hour greater than 7 days but less than or equal to 31 days is by day greater than 31 days but less than or equal to 2 years is by month greater than 2 years is by year

About viewing bar charts

In the reports that contain histograms or bar charts that involve threats, mouse over the graph bars to see the names of the threats.

About viewing the reports in Asian languages

Histograms and 3D-bar graphs are created on the server as images before the charts are sent to the browser. By default, the server that you use to create these charts looks for the MS Arial Unicode font. MS Arial Unicode is available as part of Microsoft Office and displays all supported languages correctly. If the MS Arial Unicode font is not found, the server uses the Lucida sans Unicode font.

Some reports on servers that display in an Asian language do not display chart text properly unless MS Arial Unicode is installed on the server. This problem occurs if your report includes a histogram or a 3D-bar graph. If you do not have the MS Arial Unicode font installed on the server, you can configure your server to get around this requirement. You can configure Symantec Endpoint Protection to use any Unicode-enabled font that you have that supports the languages in your environment.

To change the font used to display reports

1. Change directory to *drive*:\Program Files\ Symantec\Symantec Endpoint Protection Manager\Inetpub\Reporting\Common.
2. Open the I18nCommon.bundle configuration file with an editor.
3. Type the name of the font file that you want to use after the equal sign (=) following the SPECIAL_FONT variable. For example, if you wanted to use Arial, you would type the following:

   SPECIAL_FONT=*arial.ttf*
4. Save the file in UTF-8 format, and then close the file.
5. Make sure that the font file you type is located in the %WINDIR%\fonts directory.

About quick reports

Quick reports are predefined, customizable reports. These reports include event data collected from your management servers as well as clients that communicate with those servers. Quick reports provide information on events specific to the settings you configure for the report. You can save the report settings so that you can run the same report at a later date, and you can print and save reports.

See "Printing and saving a copy of a report" on page 257.

Quick reports are static; they provide information specific to the time frame you specify for the report. Alternately, you can monitor events in real time using the logs.

See "About logs" on page 261.

Table 12-11 describes the report types for quick reports.

Table 12-11 Quick report types

Report type	Description
Audit	The Audit report contains information about policy modification activities, such as the event times and types, policy modifications, domains, sites, administrators, and descriptions. See "About the information in the Audit report and log " on page 224.
Application and Device Control	The Application and Device Control reports contain information about events where access to a computer was blocked or a device was kept off the network. See "About the information in the Application Control and Device Control reports and logs" on page 225.

Table 12-11 Quick report types *(continued)*

Report type	Description
Compliance	The Compliance reports contain information about the Enforcer server, the Enforcer clients, the Enforcer traffic, and host compliance. See " About the information in the Compliance reports and logs " on page 226.
Computer Status	The Computer Status reports contains information about the real-time operational status of the computers in the network. See "About the information in the Computer Status reports and log" on page 227.
Network Threat Protection	The Network Threat Protection reports allow you to track a computer's activity and its interaction with other computers and networks. They record information about the traffic that tries to enter or exit the computers through their network connections. See "About the information in the Network Threat Protection reports and logs" on page 231.
Risk	The Risk reports include information about risk events on your management servers and their clients. See "About the information in the Risk reports and log" on page 235. Also included in the Risk reports are the TruScan proactive threat scan reports. See "About the information in the TruScan proactive threat scan reports and logs" on page 234.
Scan	The Scan reports provide information about antivirus and antispyware scan activity. See "About the information in the Scan reports and log" on page 238.
System	The System reports contain information that is useful for troubleshooting client problems. See "About the information in the System reports and logs" on page 239.

You can configure basic settings and advanced settings for all reports to refine the data you want to view. You can also save your custom filter with a name to run the same custom report at a later time.

Table 12-12 describes all the basic settings available for all types of quick reports.

Table 12-12 Basic filter settings for quick reports

Setting	Description
Time range	Specifies the time range of events you want to view in the report. Select from the following times: ■ **Past 24 hours** ■ **Past week** ■ **Past month** ■ **Current month** ■ **Past three months** ■ **Past year** ■ **Set specific dates** If you choose **Set specific dates**, some reports require that you set a start date and end date. Other reports require that you set the Last checkin time, which is the last time that the computer checked in with its server. The default is Past 24 hours.
Start date	Specifies the start date for the date range. Only available when you select **Set specific dates** for the time range.
End date	Specifies the end date for the date range. Only available when you select **Set specific dates** for the time range. **Note:** You cannot set an end date that is the same as the start date or earlier than the start date.
Last checkin after	Specifies that you want to see all entries that involve a computer that has not checked in with its server since this time. Only available for **Computer Status** reports when you select **Set specific dates** for the time range.
Status	Available for the **Network Compliance Status Compliance** report. Select from the following: ■ Authenticated ■ Disconnected ■ Failed ■ Passed ■ Rejected Available for the Compliance Status Compliance report. Select from the following actions: ■ Passed ■ Failed

Table 12-12 Basic filter settings for quick reports *(continued)*

Setting	Description
Group by	Many of the reports can be grouped in appropriate ways. For example, the most common choice is to view information for only one group or subnet, but some reports provide other appropriate choices.
Target	Available for the **Network Threat Protection Top Targets Attacked** report. Select from the following: ■ Group ■ Subnet ■ Client ■ Port Available for the **Network Threat Protection Attacks Over Time** report. Select from the following: ■ All ■ Group ■ IP Address ■ Operating System ■ User Name ■ Attack Type Available for the **Network Threat Protection Blocked Applications Over Time and Traffic Notifications Over Time** reports. Select from the following: ■ All ■ Group ■ IP Address ■ Operating System ■ User Name Available for the **Network Threat Protection Top Traffic Notifications** report. Select from the following: ■ All ■ Traffic ■ Packet

Table 12-12 Basic filter settings for quick reports *(continued)*

Setting	Description
X-axis **Y-axis**	Available for the **Risk Top Risk Detections Correlation** report. Select from the following: ■ Computer ■ User Name ■ Domain ■ Group ■ Server ■ Risk Name
Bin width	Specifies the width of a bin for forming a histogram. Available for the **Scan Statistics Histogram Scan** report.
Number of bins	Specifies the number of bins you want used to form the bars of a histogram. Available for the **Scan Statistics Histogram Scan**report.

The advanced settings provide additional control over the data that you want to view. They are specific to the report type and content.

For a description of each advanced setting that you can configure, you can click **Tell me more** to display the context-sensitive help for that type of report.

If you have multiple domains in your network, many reports allow you to view data for all domains, one site, or a few sites. The default for all quick reports is to show all domains, groups, servers, and so on, as appropriate for the report you select to create.

Note: If you have only Symantec Network Access Control installed, a significant number of reports are empty. The **Application and Device Control**, **Network Threat Protection**, **Risk**, and **Scan** reports do not contain data. The **Compliance** and **Audit** reports do contain data, as do some of the **Computer Status** and **System** reports.

See "Creating quick reports" on page 250.

See "About using the filters that search for groups in reports and logs" on page 257.

Creating quick reports

Generate a quick report by selecting from the basic filter settings options that appear under **What filter settings would you like to use?**. If you want to configure additional options to construct a report, click **Advanced Settings**. The basic settings and advanced settings vary from report to report.

For a description of each advanced setting, you can click **Tell me more** for that type of report on the Symantec Endpoint Protection Manager console. Clicking **Tell me more** displays the context-sensitive help for that type of report.

You can save the report settings so that you can run the same report at a later date, and you can print and save reports.

Note: The filter option text boxes that accept wildcard characters and search for matches are not case-sensitive. The ASCII asterisk character is the only asterisk character that can be used as a wildcard character.

See "Saving and deleting quick report filters" on page 252.

See "Printing and saving a copy of a report" on page 257.

See "Creating and deleting scheduled reports" on page 255.

To create a quick report

1. In the console, click **Reports**.
2. On the **Quick Reports** tab, in the **Report type** list box, select the type of report that you want to create.
3. In the **Select a report** list box, select the name of the report you want to view.

   For the **Network Compliance Status** report and the **Compliance Status** report, in the **Status** list box, select a saved filter configuration that you want to use, or leave the default filter.

   For the **Top Risk Detections Correlation** report, you can select values for the **X-axis** and **Y-axis** list boxes to specify how you want to view the report.

   For the **Scan Statistics Histogram Scan** report, you can select values for **Bin width** and **Number of bins**.

   For some reports, you can specify how to group the report results in the **Group** list box. For other reports, you can select a target in the **Target** field on which to filter report results.
4. In the **Use a saved filter** list box, select a saved filter configuration that you want to use, or leave the default filter.
5. Under **What filter settings would you like to use?**, in the **Time range** list box, select the time range for the report.

6 If you select **Set specific dates**, then use the **Start date** and **End date** list boxes. These options set the time interval that you want to view information about.

When you generate a Computer Status report and select **Set specific dates**, you specify that you want to see all entries that involve a computer that has not checked in with its server since the time you specify in the **Last checkin after** field.

7 If you want to configure additional settings for the report, click **Advanced Settings** and set the options that you want.

You can click **Tell me more** to see descriptions of the filter options in the context-sensitive help.

You can save the report configuration settings if you think you will want to run this report again in the future.

8 Click **Create Report**.

Saving and deleting quick report filters

You can save custom report settings so that you can generate the report again at a later date. When you save your settings, they are saved in the database. The name you give to the filter appears in the **Use a saved filter** list box for that type of logs and reports.

Note: The filter configuration settings that you save are available for your user logon account only. Other users with reporting privileges do not have access to your saved settings.

You can delete any report configuration that you create. When you delete a configuration, the report is no longer available. The default report configuration name appears in the **Use a saved report** list box and the screen is repopulated with the default configuration settings.

See "About duplicate filter names" on page 253.

See "About using the Past 24 hours filter in reports and logs" on page 257.

See "About using the filters that search for groups in reports and logs" on page 257.

To save a filter

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

2 On the **Quick Reports** tab, select a report type from the list box.

3 Change any basic settings or advanced settings for the report.

4 Click **Save Filter**.

5 In the **Filter name** text box, type a descriptive name for this report filter. Only the first 32 characters of the name that you give display when the filter is added to the **Use a saved filter** list.

6 Click **OK**.

7 When the confirmation dialog box appears, click **OK**.

After you save a filter, it appears in the **Use a saved filter** list box for related reports and logs.

To delete a saved filter

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

2 On the **Quick Reports** tab, select a report type.

3 In the **Use saved filter** list box, select the name of the filter that you want to delete.

4 Click the **Delete** icon beside the **Use a saved filter** list box.

5 When the confirmation dialog box appears, click **Yes**.

About duplicate filter names

Filter storage is based in part on the creator, so problems do not occur when two different users create a filter with the same name. However, a single user or two users who log on to the default admin account should not create filters with the same name.

If users create filters with the same name, a conflict can occur under two conditions:

- Two users are logged on to the default admin account on different sites and each creates a filter with the same name.
- One user creates a filter, logs on to a different site, and immediately creates a filter with the same name.

If either condition occurs before site replication takes place, the user subsequently sees two filters with the same name in the filter list. Only one of the filters is usable. If this problem occurs, it is a best practice to delete the usable filter and recreate it with a different name. When you delete the usable filter, you also delete the unusable filter.

See "Saving and deleting quick report filters" on page 252.

About scheduled reports

Scheduled reports are the reports that run automatically based on the schedule that you configure. Scheduled reports are emailed to recipients, so you must include the email address of at least one recipient. After a report runs, the report is emailed to the recipients that you configure as an .mht file attachment.

Scheduled reports are emailed to their recipients at the hour and time that the administrator configures by using the **Run every** option. The data that appears in the snapshot reports is updated in the database every hour. At the time that Symantec Endpoint Protection emails a snapshot report, the data in the report is current to within one hour. The other reports that contain data over time are updated in the database based on the upload interval that you configured for the client logs.

See "Configuring client log settings" on page 361.

Note: If you have multiple servers within a site that share a database, only the first-installed server runs the reports scheduled for the site. This default ensures that all the servers in the site do not run the same scheduled scans simultaneously. If you want to designate a different server to run scheduled reports, you can configure this option in the local site properties.

See "Editing site properties" on page 309.

The following reports are only available as scheduled reports:

- **Client Software Rollout (Snapshots)**
- **Clients Online/Offline Over Time (Snapshots)**
- **Clients With Latest Policy over Time (Snapshots)**
- **Non-Compliant Clients Over Time (Snapshots)**
- **Virus Definition Rollout (Snapshots)**

You can print and save scheduled reports, as you do with the quick reports.

Note: When you first create a scheduled report, you must use the default filter or a filter you've already saved. After you have scheduled the report, you can go back and edit the filter.

See "Editing the filter used for a scheduled report" on page 256.

For information about the options you can set in these procedures, on the **Scheduled Reports** tab, you can click **Tell me more**.

See "Creating and deleting scheduled reports" on page 255.

See "About using the filters that search for groups in reports and logs" on page 257.

Creating and deleting scheduled reports

You can add or edit scheduled reports, and you can delete scheduled reports. If you have a scheduled report that you do not want to run, you can uncheck **Enable this scheduled report** rather than deleting the report.

See "Editing the filter used for a scheduled report" on page 256.

To create a scheduled report

1. In the console, click **Reports**.
2. On the **Scheduled Reports** tab, click **Add**.
3. In the **Report name** text box, type a descriptive name and optionally, type a longer description.

   Although you can paste more than 255 characters into the description text box, only 255 characters are saved in the description.
4. If you do not want this report to run, uncheck the **Enable this scheduled report** check box.
5. Select the report type that you want to schedule from the list box.
6. Select the name of the specific report that you want to schedule from the list box.
7. Select the name of the saved filter that you want to use from the list box.
8. In the **Run every** text box, select the time interval at which you want the report to be emailed to recipients (hours, days, weeks, months). Then, type the value for the time interval you selected. For example, if you want the report to be sent to you every other day, select days and then type 2.
9. In the **Start after** text box, type the date that you want the report to start or click the calendar icon and select the date. Then, select the hour and minute from the list boxes.
10. Under **Report Recipients**, type one or more comma-separated email addresses.

    You must already have set up mail server properties for email notifications to work.
11. Click **OK** to save the scheduled report configuration.

To delete a scheduled report

1. In the console, click **Reports**.
2. On the **Scheduled Reports** tab, in the list of reports, click the name of the report that you want to delete.
3. Click **Delete**.
4. When the confirmation dialog box appears, click **Yes**.

Editing the filter used for a scheduled report

You can change the settings for any report that you have already scheduled. The next time the report runs it uses the new filter settings. You can also create additional scheduled reports, which you can associate with a previously saved report filter.

Note: When you associate a saved filter with a scheduled report, make sure that the filter does not contain custom dates. If the filter specifies a custom date, you get the same report every time the report runs.

See "About duplicate filter names" on page 253.

See "About using the Past 24 hours filter in reports and logs" on page 257.

See "About using the filters that search for groups in reports and logs" on page 257.

To edit the filter used for a scheduled report

1. In the console, click **Reports**.
2. Click **Scheduled Reports**.
3. In the list of reports, click the scheduled report that you want to edit.
4. Click **Edit Filter**.
5. Make the filter changes that you want.
6. Click **Save Filter**.

   If you want to retain the original report filter, give this edited filter a new name.
7. Click **OK**.
8. When the confirmation dialog box appears, click **OK**.

About using the Past 24 hours filter in reports and logs

If you select Past 24 hours for the time range of a report or a log view, the range begins when you select the filter. If you refresh the page, the start of the 24-hour range does not reset. If you select the filter and wait to create a report, the time range starts when you selected the filter. This condition also applies when you view an event log or alert log. The time range does not start when you create the report or view the log.

If you want to make sure the past 24-hour range starts now, select a different time range and then reselect Past 24 hours.

Note: The start of the past 24-hour time range filter on the home page is determined at the time the home page is accessed.

See "Saving and deleting quick report filters" on page 252.

About using the filters that search for groups in reports and logs

Because all groups are subgroups of the My Company parent group, when a filter searches for groups, it searches hierarchically starting with the string My Company. If the name of the group does not start with the letter m, you should precede the string that you search for with an asterisk. Or, you can begin the string with a m* when you use wildcard characters.

For example, if you have a group named Services, and you type s* into this box, no group is found and used in the view. To find a group named Services, you need to use the string *s* instead. If you have more than one group that contains the letter s, you may want to use a string such as *ser*.

See "Saving and deleting quick report filters" on page 252.

Printing and saving a copy of a report

When you generate a report, the report appears in a new window. You can print the report or save a copy of the report.

Note: By default, Internet Explorer does not print background colors and images. If this printing option is disabled, the printed report may look different than the report that you created. You can change the settings in your browser to print background colors and images.

See "About the reports you can run" on page 221.

To print a copy of a report

1. In the report window, click **Print**.
2. In the Print dialog box, select the printer you want, if necessary, and then click **Print**.

When you save a report, you save a snapshot of your security environment that is based on the current data in your reporting database. If you run the same report later, based on the same filter configuration, the new report shows different data.

To save a copy of a report

1. In the report window, click **Save**.
2. In the File Download dialog box, click **Save**.
3. In the Save As dialog box, in the Save in selection box, browse to the location where you want to save the file.
4. In the File name list box, change the default file name, if desired.
5. Click **Save**.

   The report is saved in Microsoft Web Archive format, single file (*.mht) in the location you selected.
6. In the Download complete dialog box, click **Close**.

About using SSL with the reporting functions

You can use SSL with the reporting functions for increased security. SSL provides confidentiality, the integrity of your data, and authentication between the client and the server.

For information about using SSL with the reporting functions, see the appropriate article in the Symantec Knowledge Base:

Configuring Secure Sockets Layer (SSL) to work with the Symantec Endpoint Protection reporting functions on Windows 2000

Configuring Secure Sockets Layer (SSL) to work with the Symantec Endpoint Protection reporting functions on Windows Server 2003

See "About the reports you can run" on page 221.

Important points about reporting

You should be aware of the following information when you use reports:

- Timestamps, including client scan times, in reports and logs are given in the user's local time. The reporting database contains events in Greenwich Mean Time (GMT). When you create a report, the GMT values are converted to the local time of the computer on which you view the reports.
- If managed clients are in a different time zone from the management server, and you use the **Set specific dates** filter option, you may see unexpected results The accuracy of the data and the time on both the client and the management server may be affected.
- If you change the time zone on the server, log off of the console and log on again to see accurate times in logs and reports.
- In some cases, the report data does not have a one-to-one correspondence with what appears in your security products. This lack of correspondence occurs because the reporting software aggregates security events.
- You can use SSL with the reporting functions for increased security. SSL provides confidentiality, the integrity of your data, and authentication between the client and the server.
  See "About using SSL with the reporting functions" on page 258.
- Risk category information in the reports is obtained from the Symantec Security Response Web site. Until the Symantec Endpoint Protection Manager console is able to retrieve this information, any reports that you generate show Unknown in the risk category fields.
- The reports that you generate give an accurate picture of compromised computers in your network. Reports are based on log data, not the Windows registry data.
- Report pages and log pages always display in the language that the management server was installed with. To display these pages when you use a remote console or browser, you must have the appropriate font installed on the computer that you use.
- If you get database errors when you run a report that includes a large amount of data, you might want to change database timeout parameters.
  See "Changing timeout parameters" on page 366.
- If you get CGI or terminated process errors, you might want to change other timeout parameters.

For more information, see the following document in the Symantec Knowledge Base: SAV Reporting Server or SEPM Reporting does not respond or shows a timeout error message when querying large amounts of data

The following information is important to note if you have computers in your network that are running legacy versions of Symantec AntiVirus:

- When you use report and log filters, server groups are categorized as domains. Client groups are categorized as groups, and parent servers are categorized as servers.
- If you generate a report that includes legacy computers, the IP address and MAC address fields display **None**.

Chapter 13

Viewing and configuring logs and notifications

This chapter includes the following topics:

About logs

Using the logs, you can view the detailed events that your security products generate. Logs contain event data from your management servers as well as all the clients that communicate with those servers. Because reports are static and do not include as much detail as the logs, some administrators prefer to monitor their network primarily by using logs.

You can use the default filter to view the logs, or you can configure the filter options to limit the data view. You can save a filter that you have customized so that you can use it in the future.

You may want to view logs to troubleshoot security or connectivity issues in your network. This information may also be useful for the investigation of threats or to verify the history of events.

Note: The Reports pages and the Logs pages always display in the language that the management server was installed with. To display these pages when you use a remote Symantec Endpoint Protection Manager console or browser, you must have the appropriate font installed on the computer that you use.

You can export some log event data to a comma-delimited file, and then import it into a spreadsheet application. Other log data can be exported to a dump file or a Syslog server.

See "Exporting log data" on page 277.

See "About logged events from your network" on page 197.

About log types

You can view the following types of logs from the **Monitors** page:

- **Audit**
- **Application and Device Control**
- **Compliance**
- **Computer Status**
- **Network Threat Protection**
- **TruScan Proactive Threat Scan**
- **Risk**
- **Scan**
- **System**

Note: All these logs are accessed from the **Monitors** page on the **Logs** tab.

Some types of logs are further divided into different types of content to make easier to view. For example, **Application Control and Device Control** logs include the **Application Control** log and the **Device Control** log. You can also run commands from some logs.

Note: If you have only Symantec Network Access Control installed, only some of the logs contain data; some logs are empty. The Audit log, Compliance log, Computer Status log, and System log contain data. If you have only Symantec Endpoint Protection installed, the Compliance logs and Enforcer logs are empty but all other logs contain data.

You can view information about the created notifications on the **Notifications** tab and information about the status of commands on the **Command Status** tab.

See "Viewing and filtering administrator notification information" on page 281.

See "Running commands and actions from logs" on page 274.

Table 13-1 describes the different types of content that you can view and the actions that you can take from each log.

Table 13-1 Log types

Log type	Contents and actions
Audit	The Audit log contains information about policy modification activity. Available information includes the event time and type; the policy modified; the domain, site, and user name involved; and a description. No actions are associated with this log.
Application and Device Control	The Application Control log and the Device Control log contain information about events where some type of behavior was blocked. The following Application and Device Control logs are available: ■ Application Control, which includes information about Tamper Protection ■ Device Control Available information includes the time the event occurred, the action taken, the domain and computer that were involved, the user that was involved, the severity, the rule that was involved, the caller process, and the target. You can add a file to a Centralized Exceptions Policy from the Application Control log. Available information includes the time the event occurred, the event type, the domain and group that were involved, the computer that was involved, the user that was involved, the operating system name, a description, the location, and the name of the application that was involved.

Table 13-1 Log types *(continued)*

Log type	Contents and actions
Compliance	The compliance logs contain information about the Enforcer server, Enforcer clients, and Enforcer traffic, and about host compliance. The following compliance logs are available if you have Symantec Network Access Control installed: ■ **Enforcer Server** This log tracks communication between Enforcers and their management server. Information that is logged includes Enforcer name, when it connects to the management server, the event type, site, and server name. ■ Enforcer Client Provides the information on all Enforcer client connections, including peer-to-peer authentication information. Available information includes time, each Enforcer's name, type, site, remote host, and remote MAC address, and whether or not the client was passed, rejected, or authenticated. ■ **Enforcer Traffic** (Gateway Enforcer only) Provides some information about the traffic that moves through an Enforcer appliance. Available information includes the time, the Enforcer name, the Enforcer type, and site. The information also includes the local port that was used, the direction, action, and a count. You can filter on the connection attempts that were allowed or blocked. ■ **Host Compliance** This log tracks the details of Host Integrity checks of clients. Available information includes the time, event type, domain/group, computer, user, operating system, description, and location. No actions are associated with these logs.

Table 13-1 Log types *(continued)*

Log type	Contents and actions
Computer Status	The Computer Status log contains information about the real-time operational status of the client computers in the network. Available information includes the computer name, IP address, infected status, protection technologies, Auto-Protect status, versions, definitions date, user, last check-in time, policy, group, domain, and restart required status. You can perform the following actions from the Computer Status log: ■ **Scan** This command launches an Active, Full, or Custom scan. Custom scan options are those that you have set for command scans on the Administrator-defined Scan page. The command uses the settings in the Antivirus and Antispyware Policy that applies to the clients that you selected to scan. ■ **Update Content** This command triggers an update of policies, definitions, and software from the Symantec Endpoint Protection Manager console to the clients in the selected group. ■ **Update Content and Scan** This command triggers an update of the policies, definitions, and software on the clients in the selected group. This command then launches an Active , Full, or Custom scan. Custom scan options are those that you have set for command scans on the Administrator-defined Scan page. The command uses the settings in the Antivirus and Antispyware Policy that applies to the clients that you selected to scan. ■ **Cancel All Scans** This command cancels all running scans and any queued scans on the selected recipients. ■ **Restart Client Computers** This command restarts the computers that you selected. If users are logged on, they are warned about the restart based on the restart options that the administrator configured for that computer. You can configure client restart options on the **General Settings** tab of the **General Settings** dialog box on the **Policies** tab of the **Clients** page. ■ **Enable Auto-Protect** This command turns Auto-Protect on for all the client computers that you selected. ■ **Enable Network Threat Protection** This command turns on Network Threat Protection for all the client computers that you selected. ■ **Disable Network Threat Protection** This command turns Network Threat Protection off for all the client computers that you selected. You can also clear the infected status of computers from this log.

Table 13-1 Log types *(continued)*

Log type	Contents and actions
Network Threat Protection	The Network Threat Protection logs contain information about attacks on the firewall and on intrusion prevention. Information is available about denial-of-service attacks, port scans, and the changes that were made to executable files. They also contain information about the connections that are made through the firewall (traffic), and the data packets that pass through. These logs also contain some of the operational changes that are made to computers, such as detecting network applications, and configuring software. The following Network Threat Protection logs are available: ■ Attacks Available information includes time, attack type, domain/group, computer, and client user name. Additional information available includes the severity; the direction/protocol; the local host IP/remote host IP, the location; and the number. ■ Traffic Available information includes time, event type, action, severity, direction, computer, local host IP/remote host IP, protocol, client user name, and number. ■ Packet Available information includes time, event type, action, domain, direction, computer, local host IP, local port, and remote host IP. No actions are associated with these logs.
TruScan Proactive Threat Scan	The TruScan Proactive Threat Scan log contains information about the threats that have been detected during proactive threat scanning. TruScan proactive threat scans use heuristics to scan for any behavior that is similar to virus and security risk behavior. This method can detect unknown viruses and security risks. Available information includes items such as the time of occurrence, event actual action, user name, computer/domain, application/application type, count, and file/path. You can add a detected process to a preexisting Centralized Exceptions Policy from this log.
Risk	The Risk log contains information about risk events. Available information includes the event time, event actual action, user name, computer/domain, risk name/source, count, and file/path. You can take the following actions from this log: ■ Add Risk to Centralized Exceptions Policy ■ Add File to Centralized Exceptions Policy ■ Add Folder to Centralized Exceptions Policy ■ Add Extension to Centralized Exceptions Policy ■ Delete from Quarantine

Table 13-1 Log types *(continued)*

Log type	Contents and actions
Scan	The Scan log contains information about antivirus and antispyware scan activity. Available information includes items such as the scan start, computer, IP address, status, duration, detections, scanned, omitted, and domain. No actions are associated with these logs.
System	The system logs contain information about events such as when services start and stop. The following system logs are available: ■ Administrative Available information includes items such as event time and event type; the domain, site, and server involved; severity; administrator; and description. ■ Client-Server Activity Available information includes items such as event time and event type; the domain, site, and server involved; client; and user name. ■ Server Activity Available information includes items such as event time and event type; the site and server involved; severity; description; and message. ■ Client Activity Available information includes items such as event time, event type, event source, domain, description, site, computer, and severity. ■ Enforcer Activity Available information includes items such as event time, event type, enforcer name, enforcer type, site, severity, and description. No actions are associated with these logs.

Viewing logs

You can generate a list of events to view from your logs that are based on a collection of filter settings that you select. Each log type and content type have a default filter configuration that you can use as-is or modify. You can also create and save new filter configurations. These new filters can be based on the default filter or on an existing filter that you created previously. If you save the filter configuration, you can generate the same log view at a later date without having to configure the settings each time. You can delete your customized filter configurations if you no longer need them.

See "Saving and deleting filters" on page 270.

Note: If database errors occur when you view the logs that include a large amount of data, you might want to change the database timeout parameters.

See "Changing timeout parameters" on page 366.

If you get CGI or terminated process errors, you might want to change other timeout parameters.

You can get more information about additional timeout parameters. See the Symantec knowledge base article "Reporting server does not report or shows a timeout error message when querying large amounts of data."

Because logs contain some information that is collected at intervals, you can refresh your log views. To configure the log refresh rate, display the log and select from the **Auto-Refresh** list box at the top right on that log's view.

Note: If you view log data by using specific dates, the data stays the same when you click **Auto-Refresh**.

For a description of each configurable option, you can click **Tell me more** for that type of report on the Symantec Endpoint Protection Manager console. Clicking **Tell me more** displays the context-sensitive help.

Note: The filter option fields that accept wildcard characters and search for matches are not case-sensitive. The ASCII asterisk character is the only asterisk character that can be used as a wildcard character.

To view a log

1. In the main window, click **Monitors**.
2. On the **Logs** tab, from the **Log type** list box, select the type of log that you want to view.
3. For some types of logs, a **Log content** list box appears. If it appears, select the log content that you want to view.
4. In the **Use a saved filter** list box, select a saved filter or leave the value **Default**.
5. Select a time from the **Time range** list box or leave the default value. If you select **Set specific dates**, then set the date or dates and time from which you want to display entries.

6 Click **Advanced Settings** to limit the number of entries you display.

You can also set any other available **Advanced Settings** for the type of log that you selected.

See "Advanced filter settings for logs and reports" on page 273.

7 After you have the view configuration that you want, click **View Log**.

The log view appears in the same window.

Displaying event details in logs

You can display details about the events that are stored in the logs.

See "Viewing logs" on page 267.

To display event details

1 In the main window, click **Monitors**.

2 On the **Logs** tab, from the **Log type** list box, select the type of log that you want to view.

3 For some types of logs, a **Log content** list box appears. If it appears, select the log content that you want to view.

4 Click **View Log**.

5 Click the event that you want to view the details of, and then click **Details**.

Viewing logs from other sites

If you want to view the logs from another site, you must log on to a server at the remote site from the Symantec Endpoint Protection Manager console. If you have an account on a server at the remote site, you can log on remotely and view that site's logs.

If you have configured Replication Partners, you can choose to have all the logs from the Replication Partners copied to the local partner and vice versa.

See "Replicating logs" on page 378.

If you choose to replicate logs, by default you see the information from both your site and the replicated sites when you view any log. If you want to see a single site, you must filter the data to limit it to the location you want to view.

Note: If you choose to replicate logs, be sure that you have sufficient disk space for the additional logs on all the Replication Partners.

To view the logs from another site

1. Open a Web browser.
2. Type the server name or IP address and the port number, 9090, in the address text box as follows:

   http://*192.168.1.100*:9090

   The console then downloads. The computer from which you log on must have the Java 2 Runtime Environment (JRE) installed. If it does not, you are prompted to download and install it. Follow the prompts to install the JRE.

   See "Logging on to the Symantec Endpoint Protection Manager console" on page 37.
3. In the console logon dialog box, type your user name and password.
4. In the **Server** text box, if it does not fill automatically, type the server name or IP address and port number 8443 as follows:

   http://*192.168.1.100*:8443
5. Click **Log On**.

Saving and deleting filters

You can construct custom filters by using the **Basic Settings** and **Advanced Settings** to change the information that you want to see. You can save your filter settings to the database so that you can generate the same view again in the future. When you save your settings, they are saved in the database. The name you give to the filter appears in the **Use a saved filter** list box for that type of logs and reports.

Note: If you selected **Past 24 hours** as the time range for a log filter, the 24-hour time range begins when you first select the filter. If you refresh the page, the start of the 24-hour range does not reset. If you select the filter, and wait to view a log, the time range starts when you select the filter. It does not start when you view the log.

If you want to make sure the past 24-hour range starts now, select a different time range and then reselect **Past 24 hours**.

To save a filter

1. In the main window, click **Monitors**.
2. On the **Logs** tab, select the type of log view that you want to configure a filter for from the **Log type** list box.

3 For some types of logs, a **Log content** list box appears. If it appears, select the log content that you want to configure a filter for.

4 In the **Use a saved filter** list box, select the filter that you want to start from. For example, select the default filter.

5 Under **What filter settings would you like to use**, click **Advanced Settings**.

6 Change any of the settings.

7 Click **Save Filter**.

8 In the dialog box that appears, in the **Filter name** box, type the name that you want to use for this log filter configuration. Only the first 32 characters of the name that you give display when the saved filter is added to the filter list.

9 Click **OK** and your new filter name is added to the **Use a saved filter** list box.

10 When the confirmation dialog box appears, click **OK**.

To delete a saved filter

1 In the **Use a saved filter** list box, select the name of the log filter that you want to delete.

2 Beside the **Use a saved filter** list box, click the **Delete** icon.

3 When you are prompted to confirm that you want to delete the filter, click **Yes**.

About duplicate filter names

Filter storage is based in part on the creator, so problems do not occur when two different users create a filter with the same name. However, a single user or two users who log into the default admin account should not create filters with the same name.

If users create filters with the same name, a conflict can occur under two conditions:

- Two users are logged into the default admin account on different sites and each creates a filter with the same name.
- One user creates a filter, logs into a different site, and immediately creates a filter with the same name.

If either condition occurs before site replication takes place, the user subsequently sees two filters with the same name in the filter list. Only one of the filters is usable. If this problem occurs, it is a best practice to delete the usable filter and recreate it with a different name. When you delete the usable filter, you also delete the unusable filter.

See "Saving and deleting filters" on page 270.

Basic filter settings for logs and reports

Most logs have the same basic settings.

Table 13-2 describes the basic settings that are common to most logs and reports.

Table 13-2 Basic settings for logs

Setting	Description
Log type/Report type	Specifies the type of log or report that you want to view. Select from the following types: ■ Audit ■ Application and Device Control ■ Compliance ■ Computer Status ■ Network Threat Protection ■ TruScan Proactive Threat Scan ■ Risk ■ Scan ■ System
Log content/Report content	If there is more than one log or report of that type, you can select the type of content that you want to view.
Use a saved filter	Specifies which filter that you want to use to create the view. You can use the default filter or a custom filter that you have named and saved for viewing log or report information.
Time range	Specifies the time range of events you want to view in the log or report. Select from the following times: ■ **Past 24 hours** ■ **Past week** ■ **Past month** ■ **Current month** ■ **Past three months** ■ **Past year** ■ **Set specific dates**

Table 13-2 Basic settings for logs *(continued)*

Setting	Description
Last checkin after	Only available for **Computer Status** log when you select **Set specific dates** for the time range. Specifies that you want to see all entries that involve a computer that has not checked in with its server since this time.
Advanced settings	Each log or report has some advanced settings that are specific to it. Click **Advanced Settings** and **Basic Settings** to toggle back and forth between them.

The advanced settings provide additional control over the data that you want to view. They are specific to the report type and content.

For a description of each advanced setting that you can configure, you can click **Tell me more** to display the context-sensitive help for that type of report.

See "Saving and deleting filters" on page 270.

Advanced filter settings for logs and reports

Advanced settings provide additional control over the data that you want to view. They are specific to the log or report type and content.

If you have computers in your network that are running legacy versions of Symantec AntiVirus, then when you use log or report filters, the following terminology applies:

- Legacy server groups are categorized as domains
- Legacy client groups are categorized as groups
- Legacy parent servers are categorized as servers

Note: You cannot filter on Symantec Client Firewall legacy data for Intrusion Prevention signatures. To see the signature versions that run on a computer, you can go to the **Computer Status** log or report. Select a computer that has Symantec Client Firewall installed, and then click **Details**. The **IDS version** field contains this information.

For a description of each configurable option, you can click **Tell me more** for that type of log or report on the Symantec Endpoint Protection Manager console. Click **Tell me more** to display the context-sensitive help.

See "Saving and deleting filters" on page 270.

Running commands and actions from logs

From the **Computer Status** log, you can run several commands on clients.

Note: Mac clients process only some of these commands.

See "Running commands on clients from the console" on page 76.

You can also right-click a group directly from the **Clients** page of the Symantec Endpoint Protection Manager console to run commands. The order in which commands and actions are processed on the client differs from command to command. Regardless of where the command is initiated, commands and actions are processed in the same way.

For information about the options you can set when you run commands, in the console on the **Logs** tab, you can click **Tell me more**. Clicking **Tell me more** displays the context-sensitive Help.

From the **Command Status** tab, you can view the status of the commands that you have run from the console and their details. You can also cancel a specific scan from this tab if the scan is in progress.

You can cancel all scans in progress and queued for selected clients from the **Computer Status** log. If you confirm the command, the table refreshes and you see that the cancel command is added to the command status table.

Note: If you run a scan command, and select a **Custom** scan, the scan uses the command scan settings that you configured on the **Administrator-defined Scans** page. The command uses the settings that are in the Antivirus and Antispyware Policy that is applied to the selected clients.

If you run a **Restart Client Computer** command from a log, the command is sent immediately. If users are logged on to the client, they are warned about the restart based on the restart options that the administrator configured for that client. You can configure client restart options on the **General Settings** tab of the **General Settings** dialog box on the **Policies** tab on the **Clients** page.

The following logs allow you to add exceptions to a **Centralized Exceptions** Policy:

- **Application Control** log
- **TruScan Proactive Threat Scan** log
- **Risk** log

See "Creating centralized exceptions from log events" on page 587.

To add any type of exception from a log, you must already have created a **Centralized Exceptions** Policy.

See "Configuring a Centralized Exceptions Policy" on page 579.

From the **Risk** log, you can also delete files from the **Quarantine**.

If Symantec Endpoint Protection detects risks in a compressed file, the compressed file is quarantined as a whole. However, the **Risk** log contains a separate entry for each file in the compressed file. You cannot use the **Delete from Quarantine** command from the **Risk** log to delete only the infected files from the **Quarantine**. To successfully delete the risk or risks, you must select all the files in the compressed file before you use the **Delete from Quarantine** command.

Note: To select the files in the compressed file, you must display them all in the log view. You can use the **Limit** option in the **Risk** log filter's **Advanced Settings** to increase the number of entries in the view.

To delete files from the Quarantine from the Risk log

1. Click **Monitors**.
2. On the **Logs** tab, from the **Log type** list box, select the **Risk** log, and then click **View Log**.
3. Select an entry in the log that has a file that has been quarantined.
4. From the **Action** list box, select **Delete from Quarantine**.
5. Click **Start**.
6. In the dialog box that appears, click **Delete**.
7. In the confirmation dialog box that appears, click **OK**.

To delete a compressed file from the Quarantine from the Risk log

1. Click **Monitors**.
2. On the **Logs** tab, from the **Log type** list box, select the **Risk** log, and then click **View Log**.
3. Select all entries for files in the compressed file.

   You must have all entries in the compressed file in the log view. You can use the **Limit** option under **Advanced Settings** to increase the number of entries in the view.
4. From the **Action** list box, select **Delete from Quarantine**.
5. Click **Start**.

6 In the dialog box that appears, click **Delete**.

7 In the confirmation dialog box that appears, click **OK**.

To run a command from the Computer Status log

1 Click **Monitors**.

2 On the **Logs** tab, from the **Log type** list box, select **Computer Status**.

3 Click **View Log**.

4 Select a command from the **Action** list box.

5 Click **Start**.

If there are settings choices for the command that you selected, a new page appears where you can configure the appropriate settings.

6 When you have finished configuration, click **Yes** or **OK**.

7 In the command confirmation message box that appears, click **Yes**.

8 In the **Message** dialog box, click **OK**.

If the command is not queued successfully, you may need to repeat this procedure. You can check to see if the server is down. If the console has lost connectivity with the server, you can log off the console and then log back on to see if that helps.

To view command status details

1 Click **Monitors**.

2 On the **Command Status** tab, select a command in the list, and then click **Details**.

To cancel a specific scan that is in progress

1 Click **Monitors**.

2 On the **Command Status** tab, click the **Cancel Scan** icon in the **Command** column of the scan command that you want to cancel.

3 When a confirmation that the command was queued successfully appears, click **OK**.

To cancel all in-progress and queued scans

1 Click **Monitors**.

2 On the **Logs** tab, from the **Log type** list box, select **Computer Status**.

3 Click **View Log**.

4 Select one or more computers in the list, and then select **Cancel All Scans** from the command list.

5 Click **Start**.

6 When the confirmation dialog box appears, click **Yes** to cancel all in-progress and queued scans for the selected computers.

7 When a confirmation that the command was queued successfully appears, click **OK**.

Exporting log data

You have several choices for exporting the data in your logs. You can export the data in some logs to a comma-delimited text file. You can export other logs' data to a tab-delimited text file that is called a dump file or to a Syslog server. Log data export is useful if you want to accumulate all logs from your entire network in a centralized location. Log data export is also useful if you want to use a third-party program such as a spreadsheet to organize or manipulate the data. You also might want to export the data in your logs before you delete log records.

When you export log data to a Syslog server, you must configure the Syslog server to receive those logs. To forward logs to third-party programs, you need to have the third-party program installed and on the network. For example, you can use Microsoft Excel to open the exported log files. Each field appears in a separate column, a separate log record in each line.

Note: You cannot restore the database by using exported log data.

See "Exporting log data to a comma-delimited text file" on page 280.

See "Exporting data to a Syslog server" on page 279.

See "Exporting log data to a text file" on page 277.

Exporting log data to a text file

When you export data from the logs to a text file, by default the files are placed in a folder. That folder path is *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\dump. Entries are placed in a .tmp file until the records are transferred to the text file.

If you do not have Symantec Network Access Control installed, some of these logs do not exist.

Table 13-3 shows the correspondence of the types of log data to the names of the exported log data files.

Table 13-3 Log text file names for Symantec Endpoint Protection

Log Data	Text File Name
Server Administration	scm_admin.log
Server Application Control	agt_behavior.log
Server Client	scm_agent_act.log
Server Policy	scm_policy.log
Server System	scm_system.log
Client Packet	agt_packet.log
Client Proactive Threat	agt_proactive.log
Client Risk	agt_risk.log
Client Scan	agt_scan.log
Client Security	agt_security.log
Client System	agt_system.log
Client Traffic	agt_traffic.log

Note: The log names in Table 13-3 do not correspond one-to-one to the log names that are used on the **Logs** tab of the **Monitors** page.

Table 13-4 shows the correspondence of the types of log data to the names of the exported log data files for the **Enforcer** logs.

Table 13-4 Additional log text file names for Symantec Network Access Control

Log Data	Text File Name
Server Enforcer Activity	scm_enforcer_act.log
Enforcer Client Activity	enf_client_act.log
Enforcer System	enf_system.log
Enforcer Traffic	enf_traffic.log

Note: When you export to a text file, the number of exported records can differ from the number you set in the **External Logging** dialog box. This situation arises when you restart the management server. After you restart the management server, the log entry count resets to zero, but there may already be entries in the temporary log files. In this situation, the first *.log file of each type that is generated after the restart contains more entries than the specified value. Any log files that are subsequently exported contain the correct number of entries.

Click **Help** on the **General** tab of the **External Logging for *Site*** dialog box for more information about the options you can set in this procedure.

See "Exporting log data" on page 277.

To export log data to a dump file

1. In the console, click **Admin**.
2. Click **Servers**.
3. Click the local site or remote site that you want to configure external logging for.
4. Click **Configure External Logging**.
5. On the **General** tab, select how often you want the log data to be sent to the file.
6. In the **Master Logging Server** list box, select the server that you want to send logs to.

   If you use Microsoft SQL with more than one management server connecting to the database, only one server needs to be a Master Logging Server.
7. Check **Export Logs to a Dump File**.
8. If necessary, check **Limit Dump File Records** and type in the number of entries that you want to send at a time to the text file.
9. On the **Log Filter** tab, select all of the logs that you want to send to text files.

   If a log type that you select lets you select the severity level, you must check the severity levels that you want to save. All levels that you select are saved.
10. Click **OK**.

Exporting data to a Syslog server

You can configure Symantec Endpoint Protection to send the log data from some logs to a Syslog server.

Note: Remember to configure your Syslog server to receive the log data.

For more information about the options you can set in this procedure, you can click **Help** on the **General** tab of the **External Logging for *Site*** dialog box.

See "Exporting log data" on page 277.

To export log data to a Syslog server

1. In the console, click **Admin**.
2. Click **Servers**.
3. Click the local site or remote site that you want to export log data from.
4. Click **Configure External Logging**.
5. On the **General** tab, select how often you want the log data to be sent to the file.
6. In the **Master Logging Server** list box, select the server you want to send logs to.

   If you use Microsoft SQL and have multiple management servers connected to the database, you only need one server to be the Master Logging Server.
7. Check **Enable Transmission of Logs to a Syslog Server**.
8. Configure the following fields as desired:
   - **Syslog Server**
     Type in the IP address or domain name of the Syslog server that you want to receive the log data.
   - **UDP Destination Port**
     Type in the destination port that the Syslog server uses to listen for Syslog messages or use the default.
   - **Log Facility**
     Type in the number of the log facility that you want to be used in the Syslog configuration file or use the default. Valid values range from 0 to 23.
9. On the **Log Filter** tab, select all of the logs that you want to send to text files. If a log type that you select lets you select the severity level, check the severity levels that you want to save.
10. Click **OK**.

Exporting log data to a comma-delimited text file

You can export the data in the logs to a comma-delimited text file.

See "Exporting log data" on page 277.

To export logs to a comma-delimited text file

1. In the console, click **Monitors**.
2. On the **Logs** tab, select the log that you want to export.
3. Change any **Basic Settings** or **Advanced Settings**.
4. Click **View Log**.
5. Click **Export**.
6. In the new window that appears, click the **File** menu and then click **Save As**.
7. If you are prompted to continue, click **Yes**.
8. In the **Save Web Page** window that appears, use the **Save in** list box to browse to the directory where you want to save the file.
9. In the **File name** text box, type a file name to use.
10. To save the raw data, in the **Save as** type list box, change the type to **Text File (*.txt)**.
11. Click **Save** to export the data to the file.

About using notifications

Notifications are messages about the security events that have taken place in your network. You can configure many different types of notifications to occur. Some notifications are directed at users and some notifications are directed at administrators.

You can configure the following notification actions to alert administrators or other designated individuals when a number of different security-related conditions are met:

- Send an email.
- Run a batch file or another executable file.
- Log an entry in the notifications log in the database.

See "Creating administrator notifications" on page 283.

See "Viewing and filtering administrator notification information" on page 281.

Viewing and filtering administrator notification information

You can view the information from the Notifications log in the same way that you view the information that is contained in other logs. You can filter the Notifications

log to view information about a single type of notification event at a time. You can filter your view of notifications and save the filters for future use.

You can filter notifications in the log based on the following criteria:

- **Time range**
- **Acknowledged status**
- **Notification type**
- **Created by**
- **Notification name**.

To view all notifications

1. In the console, click **Monitors**.
2. On the **Notifications** tab, click **View Notifications**.

   The list of all types of notifications appears.

To filter your view of notifications

1. In the console, click **Monitors**.
2. On the **Notifications** tab, under **What filter settings would you like to use**, click **Advanced Settings**.
3. Set any option you want to filter on.

   You can filter on any combination of the time range, the acknowledged status, the notification type, the creator, or a specific notification name.
4. Click **View Notifications**.

   A list of the type of notifications that you selected appears.

Threshold guidelines for administrator notifications

Some notification types contain default values when you configure them. These guidelines provide reasonable starting points depending on the size of your environment, but they may need to be adjusted. Trial and error may be required to find the right balance between too many and too few notifications for your environment. Set the threshold to an initial limit, then wait for a few days. See if you receive notifications too infrequently or if notifications swamp you or your network.

For virus, security risk, and firewall event detection, suppose that you have fewer than 100 computers in a network. A reasonable starting point in this network is to configure a notification when two risk events are detected within one minute.

If you have 100 to 1000 computers, detecting five risk events within one minute may be a more useful starting point.

You may also want to be alerted when clients have out-of-date definitions. You may want to be notified of each client that has a definitions file that is more than two days out of date.

See "Creating administrator notifications" on page 283.

Creating administrator notifications

You can create and configure notifications to be triggered when certain security-related events occur.

You can configure the software to take the following notification actions:

- Log the notification to the database.
- Send an email to individuals.

  Note: To send notifications by email, you must also configure a mail server. To configure a mail server, click the **Admin > Servers** page, select a server, click **Edit Server Properties**, and then click the **Mail Server** tab.

- Run a batch file or other kind of executable file.

The default damper period for notifications is **Auto** (automatic). If a notification is triggered and the trigger condition continues to exist, the notification action that you configured is not performed again for 60 minutes. For example, suppose you set a notification so that you are emailed when a virus infects five computers within one hour. If a virus continues to infect your computers at or above this rate, Symantec Endpoint Protection emails you every hour. The emails continue until the rate slows to fewer than five computers per hour.

You can configure the software to notify you when a number of different types of events occur.

See "Threshold guidelines for administrator notifications" on page 282.

Table 13-5 describes the different types of events that trigger different types of notifications.

Table 13-5 Notification types

Notification	Description
Authentication failure	Logon failures trigger this type of notification. You set the number of logon failures and the time period that you want to trigger a notification. Symantec Endpoint Protection notifies you if the number of logon failures that occur during the time period exceeds your setting. It reports the number of logon failures that occurred.
Client list changed	Changes to the clients trigger this type of notification. The types of changes that can trigger this notification include the addition, movement, name change, or deletion of a client. Additional possibilities are that a client's Unmanaged Detector status, client mode, or hardware changed.
Client security alert	You can choose from compliance, Network Threat Protection, traffic, packet, device control, and application control security events. You can also choose the type and extent of the outbreak that should trigger this notification and the time period. Types include occurrences on any computer, occurrences on a single computer, or occurrences on distinct computers. Some of these types require that you also enable logging in the associated policy.
Enforcer is down	An offline Enforcer appliance triggers this type of notification. The notification tells you the name of each Enforcers, its group, and the time of its last status.
Forced or Commercial application detected	The detection of an application on the Commercial Application List or on the administrator's list of applications to watch for triggers this notification.
New learned application	New learned applications trigger this type of notification.
New risk detected	New risks trigger this type of notification.
New software package	New software package downloads trigger this type of notification.
Risk outbreak	You set the number and type of occurrences of new risks and the time period that should trigger this type of notification. Types include occurrences on any computer, occurrences on a single computer, or occurrences on distinct computers.

Table 13-5 Notification types *(continued)*

Notification	Description
Server health	Server health statuses of offline, poor, or critical trigger this notification. The notification lists the server name, health status, reason, and last status.
Single risk event	The detection of a single risk event triggers this notification. The notification lists a number of details about the risk, which includes the user and computer involved, and the action that Symantec Endpoint Protection took.
System event	System events such as server and Enforcer activities, replication failure, backup and restore problems, and system errors trigger this notification. The notification lists the number of such events that were detected.
Unmanaged computers	Unmanaged computers trigger this notification. The notification lists details such as the IP address, MAC address, and operating system for each computer.
Virus definitions out-of-date	You define out-of-date when setting up the notification. You set the number of computers and the number of days that the computer's definitions must be older than to trigger this notification.

Using the **Notification Conditions** settings, you can configure a client security alert by occurrences on any computer, a single computer, or on distinct computers. You can also configure these options for a risk outbreak.

You may want to create a Network Threat Protection notification that is triggered when a traffic event matches the criteria that are set for a firewall rule.

To create this type of notification, you must perform the following tasks:

- In the **Firewall Policy Rules** list, check the **Send Email Alert** option in the **Logging** column of the rules you want to be notified about.
- On the **Notifications** tab, configure a Client security alert for Network Threat Protection, Packet, or Traffic events.

See "Configuring notifications for Network Threat Protection" on page 511.

For a description of each configurable option, you can click **Tell me more** on the Symantec Endpoint Protection Manager console. **Tell me more** displays the context-sensitive Help.

Note: You can filter your view of the **Notification Conditions** you have created by using the **Show notification types** list box. To be sure that the new notifications that you create are displayed, make sure that **All** is selected in this list box.

To create a notification

1. In the console, click **Monitors**.
2. On the **Notifications** tab, click **Notification Conditions**.
3. Click **Add**, and then select the type of notification that you want to add from the list that appears.
4. In the new window that appears, in the **Notification name** text box, type a descriptive name.
5. Specify the filter options that you want. For example, for some types of notifications, you can limit the notification to specific domains, groups, servers, computers, risks, or applications.
6. Specify the notification settings and the actions that you want to occur when this notification is triggered. You can click **Help** to see descriptions of the possible options for all types of notifications.

   If you select **Run the batch or executable file** as the action to take, type in the name of the file. Path names are not allowed. The batch file or executable file to run must be located in the following directory:

   drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\bin

   If you select **Send email to** as the action to take, the email notification depends on the mail server's user name option. The user name that is configured for the mail server from the **Server Properties** dialog box must be of the form *user@domain*. If this field is left blank, the notifications are sent from SYSTEM@*computer name*. If the reporting server has a name that uses Double Byte Character Set (DBCS) characters, you must specify the user name field with an email account name of the form *user@domain*.
7. Click **OK**.

To create a Network Threat Protection notification

1. In the console, click **Monitors**.
2. On the **Notifications** tab, click **Notification Conditions**.
3. Click **Add** and select **Client security alert**.
4. Type in a name for this notification.
5. If you want to limit this notification to specific domains, groups, servers, or computers, specify the filter options that you want.

6 Select one of the following outbreak types:

- Occurrences on distinct computers
- Occurrences on any computer
- Occurrences on single computer

7 To specify the type of Network Threat Protection activity, check one of the following check boxes:

- For the attacks and events that the firewall detects or the Intrusion Prevention signatures detect, check **Network Threat Protection events**.
- For the firewall rules that are triggered and recorded in the **Packet** log, check **Packet events**.
- For the firewall rules that are triggered and recorded in the **Traffic** log, check **Traffic events**.

8 If desired, change the default notification conditions to set the number of occurrences within the number of minutes that you want to trigger this notification.

9 Check **Send email to**, and then type in the email addresses of the people that you want to notify when these criteria are met.

10 Click **OK**.

The **Send Email Alert** option in the **Logging** column of the **Firewall Policy Rules** list is now operational. When this notification is triggered, email is sent.

See "Configuring email messages for traffic events" on page 513.

About editing existing notifications

You can edit the settings of an existing notification. Any previous entries that were generated from the notification display messages in the notifications log based on your new settings. If you want to retain your past notification messages in the notifications log view, do not edit the settings of an existing notification. Instead, create a new notification with a new name. Then, disable the existing notification by unchecking the actions that you configured under What should happen when this notification is triggered.

See "Creating administrator notifications" on page 283.

Chapter 14

Managing domains and administrators

This chapter includes the following topics:

Managing domains and administrator accounts

You manage domains and administrator accounts on the Admin page.

Table 14-1 Account administration

Task	Description
Decide whether to add multiple domains	Decide whether to add additional domains for multiple businesses. See "About domains" on page 290. See "Adding a domain" on page 292. See "Specifying the current domain" on page 293.
Decide who needs an account	Decide who needs to access Symantec Endpoint Protection Manager. Decide whether the access should be restricted or unrestricted. These administrators can view and manage the contents of their own domain, but they cannot view and manage the content of other domains See "About administrators" on page 293.
Create accounts	Create an account for the administrators and the users who need access to Symantec Endpoint Protection Manager. See "Adding an administrator account" on page 296.
Edit accounts	If necessary, you can edit accounts after you create them. See "Switching between an administrator and a limited administrator" on page 299.
Lock an administrator account	You can lock an administrator account after someone has tried to log on to Symantec Endpoint Protection Manager too many times. See "Locking an administrator's account after too many logon attempts" on page 300.
Reset passwords	You can perform the following tasks for passwords: ■ Reset the admin account password to **admin**. See "Resetting the administrator password to admin" on page 301. ■ Reset an administrator's password See "Changing an administrator's password" on page 303.

About domains

A domain is a structural container in the Symantec Endpoint Protection Manager console that you use to organize a hierarchy of groups, clients, computers, and

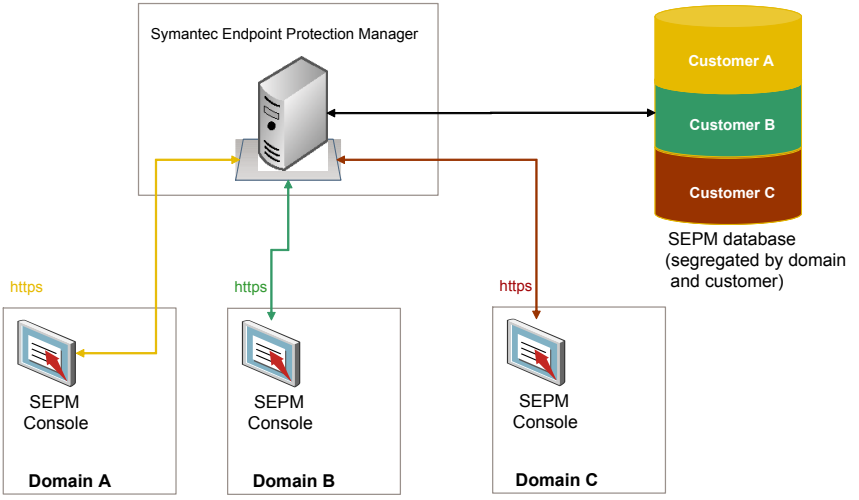
policies. You set up domains to manage your network resources. The domains in Symantec Endpoint Protection Manager do not relate to Microsoft domains.

If your company is large, with sites in multiple regions, you may need to have a single view of management information. Yet, you can delegate administrative authority, physically separate security data, or have greater flexibility in how users, computers, and policies are organized. If you are a managed service provider (MSP), you may need to manage multiple independent companies, as well as Internet service providers. To meet these needs, you can create multiple domains. For example, you can create a separate domain for each country, region, or company.

When you install a management server, the console includes one domain. Each domain that you add shares the same management server and database. Each domain provides an additional instance of the console. All data in each domain is completely separate. This separation prevents administrators in one domain from viewing data in other domains. You can add an administrator account so that each domain has its own administrator. These administrators can view and manage the contents of their own domain, but they cannot view and manage the content of other domains.

See "Adding an administrator account" on page 296.

Figure 14-1 Overview of Symantec Endpoint Protection Manager domains



When you first add the domain, the domain is empty. You must configure the domain to be the current domain. You then add groups, clients, computers, and policies to this domain.

See "Adding a domain" on page 292.

See “Specifying the current domain” on page 293.

You can copy policies and clients from one domain to another. To copy policies between domains, you export the policy from the originating domain and you import the policy into the destination domain. To copy clients between domains, you can use the SylinkDrop tool. This tool replaces the communication file on a client to allow the client to talk to a different management server. The SylinkDrop tool is located the Tools\NoSupport\Sylinkdrop folder on CD 3.

See “Exporting a policy” on page 101.

See “Recovering client communication settings by using the SylinkDrop tool” on page 188.

Adding a domain

You can add a domain if you want to use multiple domains. For example, if you manage multiple independent companies, you may want to have a separate domain for each company.

See “About domains” on page 290.

Note: You can use a domain ID for disaster recovery. If all the management servers in your organization fail, you need to rebuild the management server by using the same ID as the old server. You can get the old domain ID from the sylink.xml file on any client.

To add a domain

1. In the console, click **Admin**.
2. On the Admin page, click **Domains**.
3. Under Tasks, click **Add Domain**.
4. In the Add Domain dialog box, type a domain name and optional company name.
5. In the Contact List text box, optionally type the additional information, such as the name of the person who is responsible for that domain.
6. If you want to add a domain ID, click **Advanced** and then type the value in the text box.
7. Click **OK**.

Specifying the current domain

After you first add a new domain in the Symantec Endpoint Protection Manager Console, the domain is empty. To add new groups, clients, policies, and administrators to the domain, you must first specify which is the current domain. In the *domain name* pane, the text (Current Domain) follows the domain name. The default domain name is Default. If you have many domains, you must scroll through the View Domains list to display which domain is the current one.

If you logged on to the console as a system administrator, you can see all domains no matter which domain is the current one. But you can only see the administrators and limited administrators that were created in the current domain. If you logged on to the console as either an administrator or a limited administrator, you only see the domain to which you have access.

If you remove the current domain, the management server logs you out. You can only remove a domain if it is not the current domain and not the only domain.

To specify the current domain

1. In the console, click **Admin**.
2. On the Admin page, click **Domains**.
3. Add and then select a new domain.

   See "Adding a domain" on page 292.
4. Under Tasks, click **Administer Domain**.
5. In the Administer Domain dialog box, to confirm, click **Yes**.
6. Click **OK**.

About administrators

You use administrators to manage your company's organizational structure and network security. For a small company, you may only need one administrator. For a large company with multiple sites and domains, you would need multiple administrators, some of whom have more access rights than others.

To help you manage the network, the Symantec Endpoint Protection Manager console provides the following types of administrator roles: system administrator, administrator, and limited administrator.

The system administrator is the super administrator of a network. System administrators can view and modify the entire organization. An administrator and a limited administrator are both one level lower than a system administrator. An administrator can view and manage all the tasks within one domain only. A

limited administrator can only manage certain tasks within the domain. For example, a limited administrator can only manage a limited number of groups within a domain.

Table 14-2 lists the responsibilities for each administrator role.

Table 14-2 Administrator types roles and responsibilities

Administrator role	Responsibilities
System administrator	A system administrator can perform the following tasks: ■ Manages all domains. ■ Creates and manages all other system administrator accounts, administrator accounts, and limited administrator accounts for all domains. ■ Manages the databases and management servers. ■ Manages Enforcers. ■ Can view and use all console settings.
Administrator	An administrator can perform the following tasks: ■ Manages a single domain ■ Creates and manages administrator accounts and limited administrator accounts within a single domain. These rights include notifications, security settings, group settings, and policy settings. ■ Cannot manage databases or management servers. ■ Cannot manage Enforcers. ■ Can view and use all console settings for a single domain only.

Table 14-2 Administrator types roles and responsibilities *(continued)*

Administrator role	Responsibilities
Limited administrator	A limited administrator can perform the following tasks: ■ Perform tasks within a domain but cannot manage a domain. ■ Manages the reports, runs remote commands, and configures policies for specific groups within a single domain. Limited administrators who do not have access to a specific policy and related settings cannot view or modify the policy. In addition, they cannot apply, replace, or withdraw a policy. ■ Cannot create other limited administrator accounts. Only a system administrator or an administrator can configure the rights for the limited administrator. ■ Manages the password rights for own account only. ■ Can view Home, Monitors, or Reports pages in the console only if given reporting rights.

You can define an administrator role for each type of administrator in your organization. For example, a large company may use the following types of administrators:

- An administrator who installs the management server and the client installation packages. After the product is installed, an administrator in charge of operations takes over.
- An operations administrator maintains the servers, databases, and installs patches.
- An antivirus administrator, who creates and maintains the Antivirus and Antivirus Policies and LiveUpdate Policies on the clients.
- A desktop administrator, who is in charge of security and creates and maintains the Firewall Policies and Intrusion Prevention Policies for the clients.
- A Help desk administrator, who creates reports and has read-only access to the policies. The antivirus administrator and desktop administrator read the reports that the Help desk administrator sends.

In this scenario, the administrator who install the management server and the operations administrator should be system administrators. The antivirus administrator and desktop administrator should be administrators for their domain only. The Help desk administrator should be a limited administrator.

When you install the Symantec Endpoint Protection Manager, a default system administrator that is called admin is created. You can then create an account for any administrators that you add.

See "Adding an administrator account" on page 296.

Adding an administrator account

As your network expands or changes, you may find the number of administrators insufficient to meet your needs. You can add one or more administrators. As you add an administrator, you specify the administrator's capabilities and constraints. As a system administrator, you can add another system administrator, administrator, or limited administrator. As an administrator within a domain, you can add other administrators and limited administrators, and configure their rights.

See "About administrators" on page 293.

Warning: If you create a new administrator account for yourself, you can override your own logon user name and password.

To add an administrator

1. In the console, click **Admin**.
2. On the Admin page, click **Administrators**.
3. Under Tasks, click **Add Administrator**.
4. In the Add Administrator dialog box, enter the administrator name.

   This name is the name with which the administrator logs on and by which the administrator is known within the application.
5. Optionally enter the full name of the administrator in the second text box.
6. Type and retype the password.

   The password must be six or more characters. All characters are permitted.
7. To configure the authentication method, click **Change**.

   The default value is Symantec Management Server Authentication. You can configure when the password expires for the default method, or change the authentication method.

   See "Setting up authentication for administrator accounts" on page 302.
8. Click **OK**.
9. Select one of the following administrator types:

- System Administrator
- Administrator
  Administrators can run reports on all groups. If you migrated from Symantec AntiVirus 10.x, and you want the administrator to run reports for these migrated server groups, click **Reporting Rights**.
- Limited Administrator
  See "Configuring the access rights for a limited administrator" on page 298.

10 Click **OK**.

About access rights

By default, administrators have access to all features in a single domain. They can also run reports on all groups in the domain, except for the groups that migrated from Symantec AntiVirus 10.x. You must explicitly configure reporting rights to these migrated groups.

By default, limited administrators do not have any access rights. You must explicitly configure reporting rights, group rights, command rights, and policy rights for this type of administrator.

Note: Parts of the user interface are not available to limited administrators when you restrict access rights.

When you restrict the rights, you restrict the types of logs that the limited administrator can view or manipulate on the Monitors tab. You also restrict the settings available on the Policies tab of the Clients page.

Administrators have all access rights by default except reporting rights to Symantec AntiVirus 10.x server groups. Limited administrators have no access rights by default; you must explicitly configure the rights.

Table 14-3 Types of access rights

Type of access rights	Description
Reporting rights	For administrators, specifies the server groups that run Symantec AntiVirus 10.x for which the administrator can view reports. Administrators can view all other reports. For limited administrators, specifies all the computers for which the administrator can run reports. Also specifies the server groups that run Symantec AntiVirus 10.x for which the administrator can view reports.
Group rights	For limited administrators only, specifies which groups the limited administrator can view and manage (full access), can view only (read-only access), or cannot view (no access).
Command rights	For limited administrators only, specifies which commands the limited administrator can run on the client computers. The limited administrator can only run these commands on the clients and groups that they have full access for. Command rights are only available if reporting rights or group rights are configured for the limited administrator.
Policy type rights	For limited administrators only, specifies which policies and policy-related settings the administrator can manage.

See "Configuring the access rights for a limited administrator" on page 298.

Configuring the access rights for a limited administrator

If you add an account for a limited administrator, you must also specify the administrator's access rights. You must specify access rights the limited administrator is created in a disabled state and is unable to log on to the management server.

See "About access rights" on page 297.

Note: Ensure that you grant reporting rights to limited administrators who will use Symantec Protection Center to access the Symantec Endpoint Protection Manager console. Reporting rights are required to integrate Symantec Endpoint Protection Manager with Symantec Protection Center.

See "About managing Symantec Protection Center accounts" on page 47.

To configure the rights for a limited administrator

1. In the console, click **Admin**.
2. On the **Admin** page, click **Administrators**.
3. Select a limited administrator.

   You can also configure the access rights when you create a limited administrator account.

   See "Adding an administrator account" on page 296.
4. Under **Tasks**, click **Edit Administrator Properties**, and then click **Access Rights**.
5. On the **Access Rights** tab, make sure that Limited Administrator is selected, and do one of the following actions:
   - Check **View reports**, and then click **Reporting Rights**.
   - Check **Manage groups**, and then click **Group Rights**.
   - Check **Remotely run commands**, and then click **Command Rights**.
   - Check **Manage policies**, and then click **Policy Type Rights**.
     You can authorize the administrator to create only non-shared policies for a location by checking **Only allow location-specific policy editing**.
6. Click **OK**.

Switching between an administrator and a limited administrator

You can change an administrator to a limited administrator, and you can change a limited administrator to an administrator. You might want to change the administrator type if responsibilities for your administrators change. For example, you might want a limited administrator to be able to create other administrator accounts. Or, you might want to switch an administrator to a limited administrator to limit the access rights.

To switch between an administrator and limited administrator

1. In the console, click **Admin**.
2. On the Admin page, click **Administrators**.
3. Under View Administrators, select the administrator.
4. Under Tasks, click **Edit Administrator Properties**, and then click **Access Rights**.
5. On the Access Rights tab, do one of the following tasks:
   - Click **Administrator**.
     If you migrated from Symantec AntiVirus 10.x, and you want the administrator to run reports for these migrated server groups, click **Reporting Rights**.
   - Click **Limited Administrator**.
     Configure the rights for the limited administrator.
6. Click **OK**.

Locking an administrator's account after too many logon attempts

You can lock the administrator's account after a certain number of logon attempts. You can also configure the management server to send an email message to the administrator about the locked account. The notification can alert the administrator that another user tried to logon with the administrator's credentials.

By default, administrator accounts are locked after 5 logon attempts. The logon attempts value is reset to 0 after the administrator successfully logs on and later logs off.

The administrator has the full number of attempts to log on again at a later time. After the administrator reaches the limit for unsuccessful logon attempts, the account is locked. The administrator must then wait for the specified number of minutes before trying to log on again.

To lock an administrator's account after too many logon attempts

1. In the console, click **Admin**.
2. On the Admin page, click **Administrators**.
3. Under View Administrators, select the administrator.
4. Under Tasks, click **Edit Administrator Properties**.

5 On the General tab, in the Email text box, type the administrator's email address.

The management server sends an email message to this email address when the management server locks the administrator's account. You must check the **Send email alert when account is locked** check box to send the email message.

6 Under Log On Attempt Threshold, move the slider to set the number of permitted incorrect logon attempts.

7 To lock the account when the administrator has exceeded the number of logon attempts, click **Lock this account when log on attempts exceed the threshold**.

8 Check or uncheck **Send an email alert when the account is locked**, and then set the number of minutes.

9 Click **OK**.

Resetting the administrator password to admin

You can use the resetpass.bat to reset the password for the Symantec Endpoint Protection Manager admin account.

Note: If you change the admin account name to something other than `admin` and then subsequently run resetpass.bat, it changes the account name back to `admin`.

See "Adding an administrator account" on page 296.

To reset the administrator password

1 Open Windows Explorer on the computer that runs Symantec Endpoint Protection Manager.

2 Locate the `<Drive>:\Program Files\Symantec\Symantec Endpoint Protection Manager\Tools` folder.

3 Double-click the `resetpass.bat` executable file.

The password is reset to `admin`.

4 Change the password immediately.

Warning: Do not use the "admin" account when setting up Active Directory Authentication. You must use a new Administrator account to use Active Directory authentication. For more information, see the Symantec Technical Support Knowledge Base article, How to setup a SEPM administrator account to use your Active Directory authentication.

Setting up authentication for administrator accounts

When you add an administrator, you can specify which authentication method the management server uses to authenticate administrator accounts.

You can authenticate administrators by using the management server with RSA SecurID. You must verify that you have an existing RSA Server and have already installed and configured the RSA SecurID server on a separate computer. Also verify that the RSA SecurID server can communicate with the SecurID Agent.

You can enable RSA security for administrator accounts on Symantec Endpoint Protection Manager.

The following RSA log on mechanisms are supported:

- RSA SecurID token (not software RSA tokens)
- RSA SecurID card
- RSA keypad card (not RSA smart cards)

To set up authentication for administrator accounts

1. Add an administrator account.

   See "Adding an administrator account" on page 296.

2. On the Administrators page, under View Administrators, select the administrator.
3. Under Tasks, click **Edit Administrator Properties**, and then click **Authentication**.
4. On the Authentication tab, select one of the following authentication options that you want to use to authenticate the administrator's account:

   - Symantec Management Server Authentication, and then select when the authentication password should expire.
     See "Adding directory servers" on page 319.
   - RSA SecurID Authentication
     See "Configuring Symantec Endpoint Protection Manager to use RSA SecurID Authentication" on page 334.

- Directory Authentication
  Then type the directory server and the administrator's account name.

5 Click **OK**.

Renaming an administrator account

To change organizational responsibilities or assignments, you may want to change the name that you have given to an administrator account.

To rename an administrator account

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

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

3 Under View Administrators, select the administrator to rename.

4 Under Tasks, click **Rename Administrator**.

5 In the Rename Administrator for *name* dialog box, change the account name.

6 Click **OK**.

Changing an administrator's password

For security purposes, you may need to change an administrator's password.

When you configure the management server in the Management Server Configuration Wizard, you select a simple or an advanced installation. If you select the simple installation, the password you enter is the same as the encryption password. If you change the administrator's password, the encryption password does not change.

To change an administrator's password

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

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

3 Under View Administrators, select the administrator.

4 Under Tasks, click **Change Administrator Password**.

5 Enter and confirm the new password.

The password must be six or more characters in length, and all characters are permitted.

6 Click **OK**.

Section 2

Advanced administrative tasks

Chapter 15

Managing sites

This chapter includes the following topics:

About site management

Symantec Endpoint Protection organizes installations of components into sites. A site comprises single or multiple management servers and one database (MS SQL or embedded). It optionally includes one or more Enforcers that are typically located together at the same business location. Large enterprise corporations typically install many sites. The number of sites that are needed may be related to the company having multiple physical locations, separate divisions, and areas on different subnets. Corporate management and IT departments are typically responsible for determining the number and location of these sites.

The local site is the Symantec Endpoint Protection Manager console that you are logged on to. However, it does not necessarily mean that the site is physically local. This site can be located in another city. Remote sites are the sites linked to the local site as a replication partner.

You can centrally manage network security from any console where you can manage both local sites and remote sites.

For both local and remote sites, you can perform the following tasks from a particular site:

- Change a site description.
  See "Editing site properties" on page 309.
- Set the console to log off after some period of time.
  See "Editing site properties" on page 309.
- Clear the clients that have not connected for a while.
  See "Editing site properties" on page 309.
- Set up log thresholds.
- Schedule daily and weekly reports.
- Configure external logging to filter and send logs to a file or to a Syslog server.
- Change a database name and description.
  See "Editing the name and description of a database" on page 354.

From a particular site, you can perform the following tasks only for a local site:

- Back up the local site immediately.
  See "Backing up a Microsoft SQL database" on page 346.
  See "Backing up an embedded database" on page 351.
- Change the backup schedule.
  See "Scheduling automatic database backups" on page 351.
- Delete a selected server (only if you have multiple management servers connected to a single Microsoft SQL database).
- Add a connection to a replication partner in the same site.
  See "Adding and disconnecting a replication partner" on page 374.
- Update the server certificate.
  See "About server certificate types" on page 337.
- Query the database for information.

These lists are not complete. They are meant to give you an idea of the types of tasks that you can perform locally or remotely.

You cannot perform some tasks from a remote site. If you want to install a new site, you need to go to a specific computer on which you installed a management server or an Enforcer. However, you can log onto a site remotely to perform other tasks that can only be performed on the console of a local site.

See "Logging on to the Symantec Endpoint Protection Manager console" on page 37.

About site replication across different company sites

After the installation of the first site at a company, you can install additional sites as replication partners. You can add replication partners when installing the second and subsequent sites.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for more information on how to configure the first site during the initial installation.

About remote sites

You can view other sites from the Servers tab. If you are connected to the other Symantec Endpoint Protection Manager consoles, you can also edit server properties of the remote site. You can perform the following tasks on remote sites:

- Delete a remote site and its replication partners.
- Change the remote server description.
- Change access to the remote site's console.
- Set up an email server for a remote site.
- Schedule directory server synchronization for a remote site.
- Set up a connection from the remote site's server to a proxy server.
- Configure external logging to send logs to a file or a Syslog server.

Editing site properties

Site properties include the following:

- Site name and site description
- Specifying the time period for when the console times out
- Whether or not to delete the clients that have not connected after some period of time
- Whether or not application learning is turned on for the site
- Maximum log sizes that are maintained at the site
- Report scheduling

You can edit local or remote site properties from the console.

To edit site properties

1. In the console, click **Admin**.
2. In the Admin page, under Tasks, click **Servers**.
3. In the Admin page, under View, expand **Local Site** (*site name*) or expand **Remote Sites**.
4. Select the site whose properties you want to edit.
5. In the Admin page, under Tasks, click **Edit Site Properties**.
6. In the Site Properties dialog box on the General tab, edit the description for the site in the Description box.

   You can use up to 1024 characters.
7. In the Site Properties dialog box on the General tab, select a value from 5 minutes to Never from the Console Timeout list.

   The default is one (1) hour. The administrator is automatically logged off the console when the Console Timeout period is reached.
8. In the Site Properties dialog box on the General tab, check **Delete clients that have not connected for *x* days**.

   You can delete the users that have not connected for a specified number of days (from 1 to 99999). The default setting is enabled for a period of thirty (30) days.
9. In the Site Properties dialog box on the General tab, check **Keep track of every application that the clients run**.

   Learned applications help administrators track a client's network access and the use of applications by recording all applications that are started on each client. You can enable or disable the learning of applications for a specific site. If this option is not enabled, then tracking of applications does not occur for that site. Tracking of applications also no longer occurs even if it is enabled for those clients that connect to the designated site. This option functions like a master switch.
10. In the Site Properties dialog box on the General tab, select a reporting server from the Select a server to send notifications and run scheduled reports list.

    This option is only relevant if you use a Microsoft SQL database that is connected to multiple databases.
11. Click **OK**.

Backing up a site

When you back up information about a site, you perform the same task as you do when you back up a database for a site.

See "Backing up a Microsoft SQL database" on page 346.

See "Backing up an embedded database" on page 351.

To back up a site

1. In the console, click **Admin**.
2. In the Admin page, under Tasks, click **Servers**.
3. In the Admin page, under View Servers, click **localhost**.
4. In the Admin page, under Tasks, click **Edit Backup Settings**.
5. In the Backup Site for Local Site: (*Site name*) dialog box, select the name of the backup server from the Backup server list.

   By default, the pathname is Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup.

   However, you can change the name of the backup path by using one of the available backup utilities.
6. Select the number of backups that you want to retain from the Number of backups to keep list.

   You can select up to 10 backups that you can retain before a backup copy is automatically deleted.
7. Click **OK**.

Deleting remote sites

When you remove a server at a company's remote site, you need to manually delete it from all management servers. The servers are listed under Remote Sites. Uninstalling the software from one management server console does not make the icon disappear from the Servers pane on other consoles.

To delete remote sites

1. In the console, click **Admin**.
2. In the Admin page, under Tasks, click **Servers**.
3. In the Admin page, under View, click **Remote Sites**.
4. In the Admin page, under View, expand Remote Sites and select the site that you plan to delete.

5 Click **Delete Remote Site**.

In the Delete Remote Site dialog, you are prompted to confirm the deletion of the remote site:

```
Deleting remote site also removes all the

replication partnerships in which this site participates.

Are you sure you want to delete this site?
```

6 Click **Yes** to delete the remote site.

You can add back a remote site that was deleted by adding a replication partner.

Chapter 16

Managing servers

This chapter includes the following topics:

About server management

You can centrally manage all types of servers from the Admin page in the Symantec Endpoint Protection Manager Console.

The Admin page, under View Servers, lists the following groupings:

- Local Site
  The console on the local site, databases, replication partners, such as other consoles whose databases replicate, and optional Enforcers
- Remote Sites
  The console on any remote site, databases, replication partners, such as other management servers whose databases replicate, and optional Enforcers

About servers and third-party passwords

All of the servers for which you can establish a connection require you to configure third-party passwords in the Symantec Endpoint Protection Manager. The

third-party passwords are automatically saved in the database that you created when you initially installed the management server.

You are typically prompted to provide the third-party password during the configuration of the following types of servers:

- Email servers
- Directory servers
- RSA servers
- Proxy servers

Starting and stopping the management server service

When you install Symantec Endpoint Protection Manager, the last step of the Server Configuration Assistant includes a console check box (selected by default). If you leave the check box selected, the console automatically starts.

The management server runs as an automatic service. If it did not start automatically, you can start it (and later stop it) by using Services from the Administrative Tools from the Start menu.

Note: If you stop the management server service, clients can no longer connect to it. If clients are required to communicate with the management server to connect to the network, they are denied access until the management server service is restarted.

For example, a client must communicate with the management server to pass a Host Integrity check.

To start the management server service

- From a command prompt, type:

```
net start semsrv
```

To stop the management server service

- From a command prompt, type:

```
net stop semsrv
```

  You can also restart the console to start the service automatically.

Granting or denying access to remote Symantec Endpoint Protection Manager consoles

You can secure the main console by granting or denying access to those computers on which a remote console is installed. By default, all consoles are allowed access. Administrators can log on to the main console locally or remotely from any computer on the network.

In addition to globally granting or denying access, you can specify exceptions by IP address. The exception list automatically denies access if you have chosen to grant access to all remote consoles. Conversely, if you deny access to all remote consoles, you automatically grant access to all exceptions.

When you create an exception, the computer that you specified must have a static IP address. You can also create an exception for a group of computers by specifying a subnet mask. For example, you may want to allow access in all areas that you administer. However, you may want to deny access to a console that is located in a public area.

To grant or deny access to a remote console

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, select the server whose console access permission you want to change.
3. Under Tasks, click **Edit Server Properties**.
4. On the General tab, click **Granted Access** or **Denied Access**.
5. If you want to specify IP addresses of the computers that are exempt from this console access permission, click **Add**.

   Computers that you add become exceptions to those that are granted access. Access is denied to these computers. If you select Denied Access, the computers that you specify become the only ones that are allowed access. Create an exception for a single computer or a group of computers.
6. In the Deny Console Access dialog box, click one of the following options:

   - **Single Computer**
     For one computer, type the IP address.
   - **Group of Computers**
     For several computers, type both the IP address and the subnet mask for the group.

7 Click **OK**.

The computers now appear in the exceptions list. For each IP address and mask, its permission status appears.

If you change Granted Access to Denied Access or vice versa, all exceptions change as well. If you have created exceptions to deny access, they now have access.

8 Click **Edit All** to change the IP addresses or host names of those computers that appear on the exceptions list.

The IP Address Editor appears. The IP Address Editor is a text editor that lets you edit IP addresses and subnet masks.

9 Click **OK**.

10 When you finish adding exceptions to the list or editing the list, click **OK**.

Deleting selected servers

You may have uninstalled multiple installations of Symantec Endpoint Protection Manager. However, they might still display in the management server Console. In this situation, you must delete the connections.

The most common occurrence of this situation is when you use a Microsoft SQL database with multiple management servers connected to it. If one management server is uninstalled, it still appears on the other consoles. You need to manually delete the servers that are no longer connected.

To delete selected servers

1 Stop the Symantec Endpoint Protection Manager service.

See "Starting and stopping the management server service" on page 314.

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

3 In the Admin page, click **Servers**.

4 Under View Servers, expand Local Site (*site name*) and click the management server that you want to delete.

5 Click **Delete Selected Server**.

6 Click **Yes** to verify that you want to delete the selected server.

Exporting and importing server settings

You may want to export or import settings for a Symantec Endpoint Protection Manager. Settings are exported to a file in xml format.

To export server settings

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, expand Local Site (Site *site name*), and then select the management server you want to export.
3. Click **Export Server Properties**.
4. Select a location in which to save the file and specify a file name.
5. Click **Export**.

To import server settings

1. In the console, click **Admin**, and then click**Servers**.
2. Under View Servers, expand Local Site (Site *site name*), and then select the management server for which you want to import settings.
3. Click **Import Server Properties**.
4. Select the file you want to import, and then click **Import**.
5. Click **Yes** to confirm the import.

Chapter 17

Managing directory servers

This chapter includes the following topics:

About the management of directory servers

You need to configure the Symantec Endpoint Protection Manager to communicate with any directory server. You need to establish a connection between the directory servers and the management server. If you do not establish a connection, you cannot import users from an Active Directory or LDAP directory servers or synchronize with them.

Adding directory servers

With Active Directory servers, you cannot filter the users before you import data. With LDAP servers, you can filter the users before you import data. Therefore you may want to add an Active Directory server that has LDAP compatibility as an LDAP server if you need to filter the data.

After you complete adding a directory server, you may want to set up synchronization.

See "Synchronizing user accounts between directory servers and a Symantec Endpoint Protection Manager" on page 321.

To add directory servers

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, select the management server to which you want to add a directory server.
3. Under Tasks, click **Edit Server Properties**.
4. In the Server Properties for *name of site* dialog box, on the Directory Servers tab, click **Add**.
5. In the Add Directory Server dialog box, type the name for the directory server that you want to add in the Name field.
6. In the Add Directory Server dialog box, check **Active Directory** or **LDAP** as the Server Type.
7. In the Add Directory Server dialog box, type the IP address, host name, or domain name in the Server IP address or name box.

   You must type the IP address, host name, or domain name of the directory server that you want to add.
8. If you add an LDAP server, type the port number of the LDAP server in the LDAP Port box.

   You cannot change the values if you add an Active Directory server.

   The default port setting is 389.
9. If you add an LDAP server, type the LDAP BaseDN in the LDAP BaseDN box.
10. Type the user name of the authorized directory server account in the User Name box.
11. Type the password for the directory server account in the Password box.
12. If you want to connect with the directory server using Secure Sockets Layer (SSL), check **Use Secure Connection**.

    If you do not check this option, a normal unencrypted connection is used.
13. Click **OK**.

Synchronizing user accounts between directory servers and a Symantec Endpoint Protection Manager

You can configure directory servers to import and synchronize users with Symantec Endpoint Protection Manager. You must have already added the directory servers before you can synchronize the information about users.

To synchronize user accounts between directory servers and a Symantec Endpoint Protection Manager

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, select the management server to which you want to add a directory server.
3. Under Tasks, click **Edit Server Properties**.
4. In the Server Properties dialog box, click the Directory Servers tab.
5. Check **Synchronize with Directory Servers** if not already checked.

   This option is the default setting.
6. To set up the schedule for how often you want to synchronize the management server with the directory server, do one of the following actions:
   - To synchronize automatically every 24 hours, click **Auto-schedule**. The default setting is scheduled to synchronize every 86400 seconds. You can also customize the interval by editing the tomcat\etc\conf.properties file.
   - To specify how often you want to synchronize, click **Synchronize every** and specify the number of hours.
7. Click **OK**.

About importing user and computer account information from an LDAP directory server

Administrators can import information about user and computer accounts from an LDAP directory server by using the LDAP protocol.

If you plan to import information about user and accounts, you must first establish a connection between the Symantec Endpoint Protection Manager and a directory server.

See "Adding directory servers" on page 319.

You can then search for and import information about users and accounts by completing the following tasks:

- Search the LDAP server for users.
  See "Searching for users on an LDAP directory server" on page 322.
- Import the information about the user accounts.
  See "Importing users from an LDAP directory server search results list" on page 324.

Searching for users on an LDAP directory server

You need to search for users on an LDAP server when you import information about users to the management server.

To search for users on an LDAP directory server

1. In the console, click **Clients**.
2. Under View Clients, select the group into which you want to import users.
3. Under Tasks, click **Import Active Directory or LDAP Users**.
4. In the Import Active Directory or LDAP Users dialog box, type the IP address or host name in the Server box.
5. In the Import Active Directory or LDAP Users dialog box, type the port number of the LDAP server or Active Directory server in the Server Port box.

   The default port number is 389.
6. If you want to connect with the directory server using Secure Sockets Layer (SSL), click **Use Secure Connection**.

   If you do not check this option, an unencrypted connection is used.

7 List the users by clicking **List Users**.

You can also type an LDAP query to locate the names of users that you want to import in the LDAP Search Base box.

You can specify search options such as attribute=value pairs. Commas must separate the attributes.

CN	CommonName
DC	DomainComponent
L	LocalityName
ST	StateOrProvinceName
O	OrganizationName
OU	OrganizationalUnitName
C	CountryName
STREET	StreetAddress

Not all LDAP servers support all options. For example, Microsoft Active Directory does not support O.

The order in which you specify the attribute=value pairs is important because it indicates the location of the entry in the LDAP directory hierarchy.

If during the installation of a directory server, you specified a DNS-type domain name such as itsupport.sygate.com, you can query a directory server, as itsupport is a typical NT NetBIOS domain name.

To query that Active Directory server, specify the LDAP search base in this order:

```
CN=Users, DC=itsupport, DC=sygate, DC=com
```

You can use wild-card characters or regular expressions in the search base. For example:

```
CN=a*, CN=Users, DC=itsupport, DC=sygate, DC=com
```

This query returns all the user names that start with the letter `a`.

Another example represents organizations in which you may want to perform a structural directory search, such as:

```
mycorp.com -> engineering.mycorp.com or sales.mycorp.com
```

You can specify either option contingent upon where you want to start searching the LDAP directory.

```
o=mycorp.com or o=engineering.mycorp.com
```

You can specify logical comparison using > or < in an LDAP search string.

An LDAP query that provides more than 1,000 results may fail. Be sure to set up the search base so that fewer than 1,000 users are reported.

8 Type the name of the LDAP user account in the Authorized Accounts box.

9 Type the password of the LDAP user account in the Password box.

10 Click **List Users** to display a list of users on the LDAP server.

If Only show users that are not added in any group is checked, only those users appear that have not already been added.

Importing users from an LDAP directory server search results list

You can also import users from an LDAP server search results list.

To import users from an LDAP directory server search results list

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

2 In the Group List tree, select the group to which you want to add users from the LDAP server.

Click **Add All** if you want to add all users or select specific users from the list, and then click **Add**.

3 Click the field name to sort by using that column.

You can sort the search results by field in ascending or descending order.

4 Select one or more users from the LDAP User List area.

You can use standard windows selection keys such as the Ctrl key to select non-contiguous users.

5 Click **Add** so that the names of new users appear in the group tree.

6 Repeat this process for adding users to other groups, as necessary, until you have added all new users to appropriate groups.

7 Click **Close**.

About organizational units and the LDAP server

The Symantec Endpoint Protection Manager can automatically synchronize users, computers, and the entire group structure in an organizational unit (OU) from an Active Directory or LDAP server. When imported, you can assign policies to the groups that are created. Imported organizational units cannot be modified in the console. If you need to add, delete, or modify them in any way, you must perform these tasks on the LDAP server. The management server automatically remains synchronized with the structure that is implemented on the directory server if you enable synchronization.

You can also create groups in the console and copy users into them from the OUs. The same user may exist in both the group on the management server and an OU. In this situation, the priority of the group is higher than the priority of the OU. Therefore the policy of the group applies to the user or computer.

Importing organizational units from an active or LDAP directory server

If you want to import an organizational unit or container, you must have already connected a Symantec Endpoint Protection Manager to an LDAP server.

See "Adding directory servers" on page 319.

You cannot filter any results from the Import Organizational Units dialog box. If you need to filter users, you must do so when you add the LDAP server to the management server. Active Directory servers cannot be filtered in either place.

This process may take time, depending on the number of users. An organizational unit cannot be placed in more than one group tree.

To import an organizational unit from an LDAP server

1. In the console, click **Clients**.
2. Under View Clients, select the group to which you want to add the organizational unit or Container.
3. Under Tasks, click **Import Organizational Unit or Container**.
4. Choose the domain.
5. Select the organizational unit.
6. Click **OK**.

About synchronizing organizational units

Integration and synchronization with LDAP servers and Active Directory is an optional feature of the Symantec Endpoint Protection Manager. You can import

organizational units from other servers and set up automatic synchronization of the imported OUs with the other servers.

Any changes that you made on the LDAP server do not appear immediately in the organizational unit that was imported into the management server. The latency period is dependent on the synchronization frequency. You can set the synchronization frequency by editing server properties on the console.

The name of the user still appears in the group on the console even if you had performed the following tasks:

- Copied a user from an organizational unit to a group
- Deleted that user from the LDAP server subsequently

The synchronization occurs only between the LDAP server and the organizational unit.

Chapter 18

Managing email servers

This chapter includes the following topics:

About managing email servers

If your network supports email servers, you may want to perform the following tasks after you establish communication between the Symantec Endpoint Protection Manager and the email server:

- Set up automatic email notifications for security events to be sent to administrators
- Set up automatic email notifications for security events to be sent to clients

Automatic email notifications can occur only if you establish a connection between the management server and at least one of the email servers in the network.

See "Configuring email messages for traffic events" on page 513.

Establishing communication between Symantec Endpoint Protection Manager and email servers

If you want to use email notification, you need to configure the email server on Symantec Endpoint Protection Manager.

To establish communication between Symantec Endpoint Protection Manager and email servers

1. In the console, click **Admin**, and then click **Server**.
2. Under View Servers, select the management server for which you want to establish a connection to the email server.
3. Under Tasks, click **Edit Server Properties**.
4. In the Server Properties dialog box, click the **Mail Server** tab.
5. Type the IP address, host name, or domain name of the email server in the Server Address text box.
6. Type the user name of the account on the email server in the User Name text box.

   You need to add a user name only if the email server requires authentication.
7. In the Server Properties dialog box, type the password of an account on the email server in the Password text box.

   You need to add a password only if the email server requires authentication
8. Click **OK**.

Chapter 19

Managing proxy servers

This chapter includes the following topics:

About proxy servers

You can use HTTP proxy and FTP proxy servers to help you manage LiveUpdates.

You can establish connections between the Symantec Endpoint Protection Manager and the following server types:

- HTTP proxy server
  See "Setting up a connection between an HTTP proxy server and Symantec Endpoint Protection Manager" on page 329.
- FTP proxy server
  See "Setting up a connection between an FTP proxy server and the Symantec Endpoint Protection Manager" on page 330.

Setting up a connection between an HTTP proxy server and Symantec Endpoint Protection Manager

If you support an HTTP proxy server in the corporate network, you need to connect the HTTP proxy server to Symantec Endpoint Protection Manager. You can use the HTTP proxy server to automatically download LiveUpdate contents.

To set up a connection between an HTTP proxy server and Symantec Endpoint Protection Manager

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, select the management server to which you want to connect an HTTP proxy server.
3. Under Tasks, click **Edit Server Properties**.
4. In the Server Properties dialog box, click the **Proxy Server** tab.
5. Under HTTP proxy settings, select **Use custom proxy settings** from the Proxy usage list.
6. Type the IP address of the HTTP proxy server in the Server address field.

   A valid IP address or server name of up to 256 characters.
7. Type the port number of the proxy server in the Port field.

   A valid port number ranges from 0 - 65535.
8. Check **Authentication needed to connect through proxy server**.
9. Type the user name of the proxy server in the User name field.
10. Type the password of the proxy server to which you want to connect in the Password field.
11. Click **OK**.

Setting up a connection between an FTP proxy server and the Symantec Endpoint Protection Manager

You can use the HTTP proxy server to automatically download LiveUpdate contents.

To set up a connection between an FTP proxy server and Symantec Endpoint Protection Manager

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, select the management server to which you want to connect an FTP proxy server.
3. Under Tasks, click **Edit Server Properties**.
4. In the Server Properties dialog box, click the **Proxy Server** tab.
5. Under FTP proxy settings, select **Use custom proxy settings** from the Proxy usage list.

6 Type the IP address of the FTP proxy server in the Server address field.

The IP address or server name can contain up to 256 characters.

7 Type the port number of the proxy server in the Port field.

A valid port number ranges from 0 - 65535.

8 Click **OK**.

Chapter 20

Managing RSA servers

This chapter includes the following topics:

About prerequisites for using RSA SecurID with the Symantec Endpoint Protection Manager

If you want to authenticate administrators that use the Symantec Endpoint Protection Manager with RSA SecurID, you need to enable encrypted authentication by running the RSA installation wizard.

Before you run the wizard, make sure that:

- You have an RSA ACE server installed
- The computer on which you installed the management server is registered as a valid host on the RSA ACE server
- Create the Node Secret file for the same host
- The sdconf.rec file on the RSA ACE server is accessible on the network
- A synchronized SecurID card or key fob has been assigned to a management server account. The logon name must be activated on the RSA ACE server
- The administrator has the RSA PIN or password available

Symantec supports the following types of RSA logons:

- RSA SecurID token (not software RSA tokens)
- RSA SecurID card
- RSA keypad card (not RSA smart cards)

To log on to the management server with the RSA SecurID, the administrator needs a logon name, the token (hardware), and a pin number.

Configuring Symantec Endpoint Protection Manager to use RSA SecurID Authentication

If your corporate network includes an RSA server, you need to install the software for an RSA ACE Agent on the computer on which you installed Symantec Endpoint Protection Manager and configure it as a SecurID Authentication client.

To configure Symantec Endpoint Protection Manager to use RSA SecurID authentication

1. Install the software for the RSA ACE Agent on the same computer on which you installed the management server. You can install the software by running the Windows .msi file from the RSA Authentication Agent CD.
2. Copy the nodesecret.rec, sdconf.rec, and agent_nsload.exe files from the RSA ACE server to the computer on which you installed the management server.
3. At the command prompt, type the following command:

   `agent_nsload -f nodesecret.rec -p` ***password for the nodesecret file***
4. In the console, click **Admin**, and then click **Servers**.
5. Under View Servers, select the management server to which you want to connect an RSA server.
6. Under Tasks, click **Configure SecurID authentication**.
7. In the Welcome to the Configure SecurID Authentication Wizard panel, click **Next**.
8. In the Qualification panel of the Configure SecurID Authentication Wizard panel, read the prerequisites so that you can meet all the requirements.
9. Click **Next**.
10. In the Upload RSA File panel of the Configure SecurID Authentication Wizard panel, browse for the folder in which the sdconf.rec file resides.

    You can also type the path name.

11 Click **Next**.

12 Click **Test** to test your configuration.

13 In the Test Configuration dialog box, type the user name and password for your SecurID, and then click **Test**.

It now authenticates successfully.

Specifying SecurID Authentication for a Symantec Endpoint Protection Manager administrator

You can specify that administrators must first be authenticated by SecurID before they can log into the management console.

You can create a new administrator or modify the settings for an existing administrator. The procedure here describes how to specify the authentication for a new administrator.

See "Adding an administrator account" on page 296.

To create a SecurID authentication for a Symantec Endpoint Protection Manager administrator

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

2 Under Tasks, click **Add Administrator**.

3 In the Add Administrator dialog box, type the name of a user that you previously configured for the RSA ACE client.

4 Next to Authentication Type, click **Change**.

5 In the Administrator Authentication dialog box, select **RSA SecurID Authentication**, and then click **OK**.

6 In the Add Administrator dialog box, click **OK**.

Configuring the management server to support HTTPS communication

If you plan to use HTTPS communication and SSL authentication between clients, management servers, and optional Enforcers, you need to add an SSL certificate. You need to add the SSL certificate to Microsoft's Internet Information Server (IIS).

You need to complete the following tasks, in this order:

- Generate or purchase an SSL certificate.

- Add the certificate to the IIS server that is installed on the same computer as the management server.
- Configure the management server lists to support HTTPS communication.

To add the certificate to the IIS server

1. Click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Under the local computer, select Symantec Web Server under Web Sites.
3. Right-click **Symantec Web Server**, and choose Properties.
4. On the Directory Security tab, click **Server Certificate** to start the Web Server Certificate Wizard.
5. Create or import a server certificate by following the steps in the wizard.

   For more information, see the IIS online Help.
6. On the Web Site tab, specify the port number for the SSL port, which is 443 by default.

Chapter 21

Managing server certificates

This chapter includes the following topics:

About server certificate types

Digital certificates are the industry standard for authenticating and encrypting sensitive data. If you want to prevent the reading of information as it passes through routers in the network, you need to encrypt the data. Therefore you need a digital certificate that uses the HTTPS protocol.

As part of this secure procedure, the server identifies and authenticates itself with a server certificate. Symantec uses the HTTPS protocol for the communication between all the servers, clients, and optional Enforcers in a network.

You must also enable encryption on Symantec Endpoint Protection Manager so that the server identifies and authenticates itself with a server certificate. If you do not enable this option, then the installation of a digital certificate is not effective.

The management server supports the following types of certificate:

- JKS keystore file (.jks)
  A Java tool that is called keytool.exe generates the keystore file. Symantec supports only the Java Key Standard (JKS) format. The Java Cryptography

Extension (JCEKS) format requires a specific version of the Java Runtime Environment (JRE). The management server supports only a JCEKS keystore file that is generated with the same version as the Java Development Kit (JDK) on the management server.
The keystore must contain both a certificate and a private key. The keystore password must be the same as the key password. It is usually exported from Internet Information Services (IIS).

- PKCS12 keystore file (.pfx and .p12)
- Certificate and private key file (DER and PEM format)
  Symantec supports unencrypted certificates and private keys in the DER or the PEM format. PKCS8-encrypted private key files are not supported.

You may want to back up the information about the certificate as a safety precaution. If the management server is damaged or you forget the keystore password, you can easily retrieve the password.

See "Locating the keystore password" on page 341.

For information about setting up server certificates, see the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*.

See "Updating a server certificate" on page 338.

See "Backing up a server certificate" on page 340.

Updating a server certificate

You can use the Update Server Certificate Wizard to guide you through the process of updating certificates.

To update a JKS server certificate

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, click the management server for which you want to update the server certificate.
3. Under Tasks, click **Manage Server Certificate**.
4. In the Welcome to the Manage Server Certificate Wizard panel, click **Next**.
5. In the Manage Server Certificate panel, click **Update the server certificate**, and then click **Next**.
6. In the Update Server Certificate panel, click **JKS keystore file (.jks)**, and then click **Next**.

7 In the JKS Keystore panel, click **Browse** to locate the JKS keystore file (.jks) on the management server, or type the pathname for this file in the text field, and then click **Open**.

8 Type the Keystore password into the Keystore password text box.

9 Type the Keystore password into the Key password text field for the second time., and then click **Next**.

10 In the Manage Server Certificate Wizard is complete panel, click **Finish**.

In the Manage Server Certificate Wizard is complete panel, a message appears that states whether or not the server certificates was successfully added.

You must log off and restart the management server before the certificate becomes effective.

To update a PKCS12 server certificate

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

2 Under View Servers, click the management server for which you want to update the server certificate.

3 Under Tasks, click **Manage Server Certificate**.

4 In the Welcome to the Manage Server Certificate Wizard panel, click **Next**.

5 In the Manage Server Certificate panel, click **Update the server certificate**, and then click **Next**.

6 In the Update Server Certificate panel, click **PKCS12 keystore file (.pfx and .p12)**, and then click **Next**.

7 In the PKCS12 Keystore panel, click **Browse** to locate the PKCS12 keystore file (.pfx and .p12) on the management server, or type the pathname for this file in the text field, and then click **Open**.

8 In the PKCS12 Keystore panel, type the Keystore password into the Keystore password text box, and then click **Next**.

9 In the Manage Server Certificate Wizard is complete panel, click **Finish**.

In the Manage Server Certificate Wizard is complete panel, a message appears that states whether or not the server certificates was successfully added.

You must log off and restart the management server before the certificate becomes effective.

To update unencrypted server certificates and private keys (DER or PEM format)

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

2 Under View Servers, click the management server for which you want to update the server certificate.

3 Under Tasks, click **Manage Server Certificate**.

4 In the Welcome to the Manage Server Certificate Wizard panel, click **Next**.

5 In the Manage Server Certificate panel, click **Update the server certificate**, and then click **Next**.

6 In the Update Server Certificate panel, click **Certificate and private key file (DER and PEM format)**, and then click **Next**.

7 In the Certificate File panel, click **Browse** to locate the certificate (DER and PEM format) on the management server or type the pathname for this file in the Certificate path text box, and then click **Open**.

8 In the Manage Server Certificate Wizard is complete panel, click **Finish**.

In the Manage Server Certificate Wizard is complete panel, a message appears that states whether or not the server certificates was successfully added.

You must log off and restart the management server before the certificate becomes effective.

Backing up a server certificate

In case the management server is damaged, you must back up the private key as well as the files that represent the certificate.

To back up a server certificate

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

2 Under View Servers, click the management server whose server certificate you want to back up.

3 Under Tasks, click **Manage Server Certificate**.

4 In the Welcome to the Manage Server Certificate Wizard pane, click **Next**.

5 In the Manage Server Certificate panel, click **Back up the server certificate** and then click **Next**.

6 In the Back Up Server Certificate panel, type the pathname or click **Browse** to locate the folder into which you want to back up the private key, and then click **Open**.

Note that you back up the management server certificate into the same folder.

The JKS Keystore file is backed up during the initial installation. A file that is called server_*timestamp*.xml is also backed up. The JKS Keystore file includes the server's private and public key pair and the self-signed certificate.

7 In the Backup Server Certificate panel, click **Next**.

8 In the Manage Server Certificate panel, click **Finish**.

Locating the keystore password

In case of a disaster, you may need to locate the keystore password.

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

To locate the keyword password

1 Open Windows explorer and locate the folder into which you backed up the files for the certificate.

By default, the Symantec Endpoint Protection Manager backs up the certificate in the *install_directory*:\Program Files\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup directory.

2 Open the server_*timestamp*.xml file and locate the keystore password.

Chapter 22

Managing databases

This chapter includes the following topics:

About the management of databases

Symantec Endpoint Protection and Symantec Network Access Control support a Microsoft SQL or an embedded database. The embedded database is typically used for organizations with 1000 or fewer clients that connect to the Symantec Endpoint Protection Manager console. Larger organizations typically use Microsoft SQL Server for the database.

If you install an embedded database, the management server can automatically install the database. Should your company environment already support a Microsoft SQL Server, then you may want to take advantage of the existing hardware and software. Microsoft SQL Servers typically let you support a larger number of clients.

A database contains information about security and enforcement policies. In addition, all configuration settings, data about attacks, logs, and reports are also included in the database. Therefore you can monitor security breaches on the network.

The information in the database is stored in tables, also called a database schema. The schema is provided for administrators who may need it for specialized reporting.

If you need detailed information about the database schema, you can download the latest *Symantec Endpoint Protection Manager Database Schema Reference* from the Symantec Endpoint Protection documentation site.

About database naming conventions

A Microsoft SQL database uses different naming conventions than an embedded database.

You can install a Microsoft SQL database on the same computer as Symantec Endpoint Protection Manager or on a separate one. In both cases the Microsoft SQL database keeps the same name as the computer on which the Microsoft SQL database server is installed.

You can install the management server and the Microsoft SQL database on the same computer that is called PolicyMgrCorp. The database retains the same name as the computer on which it is installed. The database name appears in the tree of the Admin page under View. It also appears as the Database Address of the Microsoft SQL database in the Database Management pane.

If you use an embedded database, the name of the database is always called localhost.

The name, localhost, appears in the Admin page under View. It is also listed as the Database Address of the embedded database in the Database Management pane.

About the Management Server Configuration Wizard and Symantec Database Tools

You can back up, schedule, and edit certain database settings, such as the name of a database, from the Symantec Endpoint Protection Manager console. However, you can only restore and reconfigure databases by using the Management Server Configuration Wizard and the Symantec Database Backup and Restore utility.

You can use the Management Server Configuration Wizard to reconfigure all of the Microsoft SQL and embedded database settings.

See "About the reconfiguration of a database" on page 345.

You can use the Symantec Database Tools utility to back up, restore, and reconfigure all of the Microsoft SQL and embedded database settings.

See "About database backup" on page 345.

About database backup

When you back up a database, you create a separate copy of it. There are several reasons to back up your database regularly.

Because the size of a database increases over time, you need to regularly back up the database. Backing up databases and removing unused space from databases is a necessary step in the maintenance of a production database.

If a disaster occurs, such as data corruption or hardware failure, you can restore the latest snapshot of the database. To get a clean copy of the database, you must revert to the point before the problem occurred. Some data may need to be reentered into the database during the recovery process. However, the main structure and a majority of the data is retained by using a recent backup.

You can back up the database from the Symantec Endpoint Protection Manager console or by using the Symantec Database Backup and Restore utility. The Symantec Database Backup and Restore utility is automatically installed during the installation.

You can back up in the following ways:

- Microsoft SQL database only
  You can use the Microsoft SQL Server Enterprise Manager to set up a maintenance plan that includes automatic backups.
- Embedded or a Microsoft SQL database
  You can perform an on-demand backup and also schedule automatic backups to occur from the console.

Backups should preferably be stored on a separate disk drive. You should back up the disk drive periodically.

See "Backing up a Microsoft SQL database" on page 346.

See "Backing up an embedded database" on page 351.

About the reconfiguration of a database

You can reconfigure a Microsoft SQL database or an embedded database for the following reasons: You need to reconfigure the database in a number of different circumstances:

- The IP address or the host name of the database server was changed.
- The port of the database server through which it connects to Symantec Endpoint Protection Manager was changed.
- The name of the database was changed.

  Note: You can also change the name of the database in the management server.

  See "Editing the name and description of a database" on page 354.
- Microsoft SQL only: The name of the user who is responsible for the database was changed. If you modify the database server's user name on a database server, the management server console can no longer connect to the database server.
- The password of the user who is responsible for the database was changed. You can modify the password of the user who is responsible for the database server. If you modify the password, the management server can no longer connect to the database server.
- Microsoft SQL only: The SQL Client Path was changed. The SQL client bin folder that by default is located in C:\Program Files\Microsoft SQL Server\80\Tools\Binn was changed.
  If you changed the SQL Client Path on the Microsoft SQL database server, the console can no longer connect to the database server.
- You upgrade an embedded database to a Microsoft SQL database.

See "Reconfiguring a Microsoft SQL database" on page 354.

See "Reconfiguring an embedded database" on page 356.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*. It provides information on how to upgrade from an embedded database to a Microsoft SQL database.

Backing up a Microsoft SQL database

You can perform an on-demand backup of a Microsoft SQL database from the Symantec Endpoint Protection Manager console or the Symantec Database Backup and Restore utility. The Symantec Database Backup and Restore utility is automatically installed during the installation of the management server. You can also use the Database Maintenance Plan wizard that is included in the Microsoft SQL Server software to back up the Microsoft SQL database. The Microsoft SQL Database Maintenance Plan wizard can also help you set up a backup schedule and other maintenance tasks.

See "Backing up a Microsoft SQL database" on page 347.

See "Backing up a Microsoft SQL database with the Database Maintenance Plan wizard" on page 347.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*. It provides information on how to back up a Microsoft SQL database with the Symantec Database Backup and Restore utility.

Backing up a Microsoft SQL database

The console includes a site backup that you can use to back up and later restore the database. In addition, you can set up a maintenance plan on the Microsoft SQL Server Agent.

The following procedure includes recommended settings.

You may need to use different settings depending on the following criteria:

- The size of your organization.
- The amount of disk space you have reserved for backups.
- Any required guidelines at your company.

To back up a Microsoft SQL database on demand

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, click the icon that represents the Microsoft SQL database.
3. Under Tasks, click **Back Up Site Now**.

   This method backs up all of the site data, including the database. You can check the System log as well as the Backup folder for status during and after the backup.
4. Click **Close**.

Backing up a Microsoft SQL database with the Database Maintenance Plan wizard

The Microsoft SQL Server Enterprise Manager provides a wizard to help set up a database maintenance plan. You can use the Database Maintenance Plan wizard to manage the database and to schedule automatic backups of the Microsoft SQL database.

Note: Make sure that the SQL Server Agent is started.

Sysadmin access rights are required to run the Database Maintenance Plan wizard.

Refer to the Microsoft SQL Server documentation for details on how to maintain a Microsoft SQL Server database.

To back up a Microsoft SQL database by using the Database Maintenance Plan wizard in the Microsoft SQL Sever 2000 Enterprise Manager

1. On the SQL Server Enterprise Manager, click **Programs > Microsoft SQL Server > Enterprise Manager**.
2. Expand server name where *server name* is the name of the server on which the database is installed.
3. Double-click the **Management** folder.

   The SQL Server Agent displays a green arrow on the icon if it is already started. If it is not started, start the SQL Server Service Manager by selecting the SQL Server Agent and then right-clicking and choosing **Start**.
4. Expand **Databases**.
5. Right-click **sem5** and select **All Tasks > Maintenance Plan**.
6. On the Welcome to the Database Maintenance Plan Wizard screen, click **Next**.
7. On the Select Databases screen, select **These Databases:** and next to it check **sem5** to back up the database. Then click **Next**.
8. On the Update Data Optimization Information screen, select **Remove unused space from database files**.
9. In the When it grows beyond: text box, type **1024** or an appropriate maximum size depending on the size of your organization.

   When the database exceeds the specified size, unused space is automatically removed.
10. In the Amount of free space to remain after shrink text box, choose **20% of the data space** or another amount that is appropriate for your company needs.
11. Data is optimized weekly and an acceptable default is specified. If you want to change the schedule, click **Change**.

    In the Edit Recurring Job Schedule dialog box that appears, specify how often and at what time to remove unused space from the database and then click **OK**.
12. When you are done setting up optimization, click **Next**.
13. On the Database Integrity Check screen, click **Next** without setting this option because the management server maintains database integrity.
14. In the Specify the Database Backup Plan screen, check **Backup the database as part of the maintenance plan** and **Verify the integrity of the backup when complete**.

15 Select the media on which to store the backup.

16 Click **Change** to modify the schedule for backup.

17 In the Edit Recurring Job Schedule dialog box, after Occurs, click **Daily**.

Select the frequency with which the database needs to be backed up. Every 1 day is recommended.

18 Check **Enable Schedule**.

19 Set the time for which you want the backups to occur. You can also choose a start and end date, or No end date if applicable, and click **OK**.

20 Click **Next**.

21 In the Specify Backup Disk Directory screen, choose a backup directory by clicking **Use the backup default directory** (the path is \MSSQL\BACKUP by default) or **Use this directory**.

22 Select the directory into which you want to copy files.

The directory must be located on the same computer as the database. You need to direct the backup to a separate disk drive.

23 Check **Create a subdirectory for each database**.

24 Click **Remove files older than** and then specify a time period after which the older backups are automatically removed or deleted.

Make sure you have sufficient disk space to store backups for the time period specified and click **Next**.

25 Proceed as follows:

If you selected Automatically maintain the Sem5 database during the configuration of the database server	Continue with step 41.
If the Recovery Model dialog box displays Simple	Continue with step 41.
If the Recovery Model dialog box displays Full	Continue with step 26.

26 In the Specify the Transaction Log Backup Plan screen, check **Backup the transaction log as part of the maintenance plan**.

27 Select the media on which to store the backup.

28 Click **Change** to modify the schedule for backing up the transaction log.

The Edit Recurring Job Schedule dialog box appears.

The maximum size of the transaction log is set to 8 GB, by default. If the transaction log reaches the maximum size, it no longer functions and the database may become corrupted. (You can change the maximum size of the transaction log on the SQL Server Enterprise Manager.)

29 After Occurs, click **Daily**.

Select the frequency with which the transaction log needs to be backed up. **Every 1 day** is recommended. Be sure to check **Enable Schedule**.

30 Select the frequency at which you want the backups to occur.

The default option is recommended, Occurs every 4 hours.

31 Select a start and end date or **No end date**, if applicable and click **OK**.

32 Click **Next**.

33 On the Specify Backup Disk Directory screen, select a backup directory by clicking **Use the backup default directory** or **Use this directory**.

The default path is \MSSQL\BACKUP.

34 Select the directory into which you want to copy files.

35 Check **Create a subdirectory for each database**.

36 Click **Remove files older than**:

37 Specify a time period after which the older backups are automatically removed or deleted.

Make sure that you have sufficient disk space to store backups for the time period specified and then click **Next**.

38 On the Reports to Generate screen, check **Write report to a text file in directory**.

Specify the full path and name of the text file where you want the report to be generated.

39 Check **Delete text report files older than** and leave this set to 4 weeks.

40 Check **Send e-mail report to operator** and specify the system administrator to whom the generated report is then sent through SQL mail. If the email operator is not available, select **New Operator** and then click **Next**.

41 In the Maintenance Plan History screen, click **Next**.

You should use the default settings for Maintenance Plan History unless you need to change them.

42 In the Completing the Database Maintenance Plan History screen, type a name for the maintenance plan such as SQL Database Maintenance, and then click **Finish**.

43 When the plan is complete, view the message that the plan was created successfully and click **OK**.

Backing up an embedded database

You can perform an on-demand backup of an embedded database from the console.

Refer to the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*. It provides information on how to back up an embedded database with the Symantec Database Backup and Restore utility.

To back up an embedded database

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

2 Under View Servers, click the icon that represents the embedded database.

3 Under Tasks, click **Back Up Site Now**.

This method backs up all site data, including the database. You can check the System log as well as the Backup folder for status during and after the backup.

4 Click **Yes** when the Back Up message appears.

5 Click **Close**.

Scheduling automatic database backups

You can establish schedules for the automatic backup of both Microsoft SQL and embedded databases.

You can perform on-demand backups of databases or set up a schedule for automatic backups of Microsoft SQL and embedded databases. However, you can also use the Microsoft SQL Server's Database Maintenance Wizard to schedule automatic backups for a Microsoft SQL database. In addition, you can also use the Symantec Database Backup and Restore utility to back either a Microsoft SQL database or an embedded database.

See "Backing up a Microsoft SQL database" on page 347.

See "Backing up an embedded database" on page 351.

See "Backing up a Microsoft SQL database with the Database Maintenance Plan wizard" on page 347.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control*. It provides information on how to back up a Microsoft SQL database with the Symantec Database Backup and Restore utility.

To schedule automatic database backups

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, click the icon that represents the Microsoft SQL or embedded database and whose backup settings you want to change.
3. Under Tasks, click **Edit Backup Settings**.
4. In the Backup Site for Local Site dialog box, click **Schedule Backups**.
5. Specify the backup frequency by selecting **Hourly**, **Daily**, or **Weekly**, and then specifying one of the following options:
   - If you choose **Hourly**, in the Start Time box, specify the number of minutes after the hour that backups should occur.
   - If you choose **Daily**, in the Start Time box, specify the hour and minutes to indicate at what time each day backups should occur.
   - If you choose **Weekly**, in the Start Time box, specify the hour and minutes to indicate the time that backups should occur.
   - If you choose **Weekly**, specify the **Day of Week** to indicate the day on which backups should occur.
6. Click **OK**.

   At the scheduled time, backups occur automatically and are placed in a .zip file that is labeled with the date on which the backup occurs. The backup file is stored in a backup folder that is created in the path as specified for the server data root.

   For example, a backup file that is created on August 1, 2007 at 9:46 AM is called 2007-Aug-01_09-46-13-AM.zip.

Restoring a database

If the database no longer functions correctly, you can restore it if you previously backed it up.

To restore a database

1. Locate the latest backup file that you have. This file is in .zip format and labeled with the date. The file is stored in a backup folder that was created in the path that was specified for the server data root.
2. Set up the computer on which you want to restore the database by using one of the following strategies
   - Using another computer
     If the hardware on the previous computer failed, you need to install the operating system and the management server on the new computer. Even though you replace the database with new data, you still have to configure a database after you complete the installation.
   - Using the same computer
     If the hardware and the management server function correctly, you can restore the database on the same computer. If you experience problems, you may want to uninstall the management server, reinstall it, configure the database, and then restore the data.
3. Log off the Symantec Endpoint Protection Manager console.
4. Stop the Symantec Endpoint Protection Manager service by selecting **Start > Programs > Administrative Tools > Services**.
5. Locate the management server service and then right-click to select **Stop**.
6. Select **Start > Programs > Symantec Endpoint Protection Manager > Database Back Up and Restore**.
7. Click **Restore**, and then click **Yes** in the message that appears.
8. In the Restoring Database dialog box, select the backup that you want to use from the list.
9. Click **OK**.

   The restoration of the database takes a few minutes. The length of time it takes to complete the task depends on the size of the database, number of users, replication partners, and other criteria.
10. As soon as the restoration of the database is completed, the following message appears:

    ```
    Database has been restored successfully.
    ```
11. Click **Exit**.
12. Click **Start > Programs > Symantec Endpoint Protection Manager** if you restored the database on a different computer because you need to delete the old database server. Otherwise you have finished restoring the database.

13 Log on to the console.

14 Click **Admin**.

15 Click **Servers**.

16 In the Admin page, under Tasks, right-click the old database server and select **Delete**.

17 Reconfigure additional criteria, such as user names and password, if necessary.

See "Reconfiguring a Microsoft SQL database" on page 354.

Editing the name and description of a database

You can edit the name and description of a local or a remote database.

You can also edit the name of the database by using the Management Server Configuration Wizard.

See "Reconfiguring a Microsoft SQL database" on page 354.

To edit the name and description of a database

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

2 Under View Servers, expand **Local Site**.

3 Select the local database or expand **Remote Sites** to select the database of a remote site whose properties you want to edit.

4 Under Tasks, click **Edit Database Properties**.

5 In the Database Properties dialog box, edit the name of the database in the **Name** field.

6 In the Database Properties dialog box, edit the description of the database in the **Description** field.

7 Click **OK**.

Reconfiguring a Microsoft SQL database

You need to use the Management Server Configuration Wizard to reconfigure the Microsoft SQL database.

See "About the reconfiguration of a database" on page 345.

To reconfigure a Microsoft SQL database

1. Stop the Symantec Endpoint Protection Manager service by selecting **Start > All Programs > Administrative Tools > Services**.
2. Locate Symantec Endpoint Protection Manager and then right-click to select **Stop**.
3. Click **Start > All Programs > Symantec Endpoint Protection Manager > Management Server Configuration Wizard**.
4. In the Welcome to the Management Server Configuration Wizard screen, click **Reconfigure the management server**.
5. Click **Next** to begin the reconfiguration.
6. Edit the name of the computer on which the management server is installed in the Server name box.
7. Edit the HTTPS port number that the management server listens on in the Server port box.

   The default port number is 8443.
8. Edit the location of the server data folder or browse to the root folder where data files are located.

   The root folder includes backups, replication, and other management server files.

   The default pathname is C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data)
9. Click **Next**.
10. Click **Microsoft SQL Server**.
11. Click **Next**.
12. Type the name of the database server in the Database server box, if applicable.

    Type the IP address or host name of the database server where the SQL Server Enterprise Manager (SEM) server saves application data.
13. Type the number of the SQL server port in the SQL server port box.

    The default port number is 1433.
14. Type the name of the database in the Database Name box.

    The name of the Microsoft SQL database where application data is stored.
15. Type the name of the user in the User box

    This name represents the user who is responsible for the database.

16 Type the password in the Password field.

This password is for the database user. This field cannot be blank.

17 Type the name of the SQL client path in the SQL Client Path.

By default, the SQL client bin folder contains the bcp.exe file. For example, C:\Program Files\Microsoft SQL Server\80\Tools\Binn.

The bcp.exe file must reside on the same computer as the one on which you installed the management server. This file is part of the SQL Server client package. You must also correctly specify the Microsoft SQL Client pathname in the Management Server Configuration Wizard. If the pathname is not specified correctly or the Microsoft SQL Client package was never installed, then you cannot reconfigure the database.

18 Click **Next**.

The database is then created. This process only takes a few minutes. A database message appears during that period of time if the management server service is still running.

19 You can select to Start Symantec Endpoint Protection Manager and Start Management Console.

These options are selected by default.

20 Click **Finish**.

You completed the reconfiguration of the database. If you kept the start options selected, the console logon appears.

Reconfiguring an embedded database

You need to use the Symantec Management Server Configuration Wizard to reconfigure the database.

See "About the reconfiguration of a database" on page 345.

To reconfigure an embedded database

1 Stop the Symantec Endpoint Protection Manager service by selecting **Start > Programs > Administrative Tools > Services**.

2 Locate Symantec Endpoint Protection Manager and then right-click to select **Stop**.

3 Click **Start > Programs > Symantec Endpoint Protection Manager > Management Server Configuration Wizard**.

4 In the Welcome to the Management Server Configuration Wizard screen, click **Reconfigure the management server**.

5 Click **Next** to begin the reconfiguration.

6 Edit the name of the computer on which the management server is installed in the Server name box.

7 Edit the HTTPS port number that the management server listens on in the Server port box.

The default port number is 8443.

8 Edit the location of the server data folder or browse to the root folder where data files are located.

The root folder includes backups, replication, and other management server files.

The default pathname is C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data)

9 Click **Next**.

10 Click **Embedded database**.

11 Click **Next**.

12 Type the number of the server port in the Database server port box.

The default port number is 2638.

13 Type the password in the Password box.

This field cannot be blank.

14 Type the password again the Confirm Password box.

15 Click **Next**.

The database creation takes a few minutes. A database message appears during that period of time if the management server service is still running.

16 You can choose to Start Symantec Endpoint Protection Manager and Start Management Console.

These options are selected by default.

17 Click **Finish**.

You completed the reconfiguration of the database. If you kept the start options selected, the console logon appears.

About managing log data

You can configure a number of options to manage the logs that are stored in the database.

About log data and storage

The data from all the logs that are uploaded to the Symantec Endpoint Protection Manager console are stored in the console database.

Data is stored in two tables in the database from the following types of logs:

- **Application and Device Control**
- **Audit**
- **Enforcer**
- **Network Threat Protection**
- **System**

The data from the other logs is stored in a single table.

You can set the log options for managing the database logs that are stored in two tables.

See "Configuring log settings for the servers in a site" on page 359.

The single table that contains the other logs' data is managed by using the database maintenance options in the site properties. You can set the database maintenance options that affect the data that is stored in a single table.

See "Configuring database maintenance options for logs" on page 365.

For the logs that are stored in two tables, one table (table A) is the current log table. New log entries are written into this table. When the log threshold or expiration occurs, new log entries are stored in the second table (table B). The data remains in table A until table B reaches its threshold or the number of days that is specified in the **Expired after** field. At that time, table A is cleared completely and new entries are stored there. The information in table B remains until the switch occurs. Switching from one table to the other, also called sweeping the logs from the database, occurs automatically. The timing of the switch depends on the log settings that you set in the site properties. The process is the same regardless of whether the sweep is automatic or manual.

You can perform a manual log sweep after backing up the database, if you prefer to use this method as part of routine database maintenance.

If you allow an automatic sweep to occur, you may lose some log data if your database backups do not occur frequently enough. If you regularly perform a manual log sweep after you have performed a database backup, it ensures that you retain all your log data. This procedure is very useful if you must retain your logs for a relatively long period of time, such as a year.

Note: The manual procedure that is described in Sweeping log data from the database manually does not affect the data in the logs that are stored in a single table in the database.

Sweeping log data from the database manually

You can manually clear the logs, but this procedure is optional and you do not have to do it.

To sweep log data from the database manually

1. To prevent an automatic sweep of the database until after a backup occurs, increase the Site Properties Log Settings to their maximums.

   See "Configuring log settings for the servers in a site" on page 359.

2. Perform the backup, as appropriate.
3. On the computer where the manager is installed, open a Web browser and type the following URL:

   https://localhost:8443/servlet/ConsoleServlet?ActionType=ConfigServer&action=SweepLogs

   After you have performed this task, the log entries for all types of logs are saved in the alternate database table. The original table is kept until the next sweep is initiated.
4. To empty all but the most current entries, perform a second sweep. The original table is cleared and entries then start to be stored there again.
5. Remember to return the Site Properties Log Settings to your preferred values.

Log data from legacy clients

The Symantec Endpoint Protection reporting functions use a temporary folder, *drive*:\Symantec\Symantec Endpoint Protection Manager\Inetpub\Reporting\Temp, for several purposes. Some administrators may want to schedule their own automated tasks to periodically clean this temporary folder. If you do so, be sure that you do not delete the LegacyOptions.inc file, if it exists. If you delete this file, you lose the incoming data from legacy Symantec AntiVirus client logs.

Configuring log settings for the servers in a site

To help control disk space usage, you can configure the number of entries that are kept on the server in a site's logs. You can also configure the number of days the entries are kept. You can configure different settings for the different sites.

Note: Log information on the Symantec Endpoint Protection Manager console **Logs** tab on the **Monitors** page is presented in logical groups for you to view. The log names on the **Site Properties Log Settings** tab correspond to log content rather than to log types on the **Monitors** page **Logs** tab.

For a description of each configurable option, you can click **Tell me more** for that type of report on the console. **Tell me more** displays the context-sensitive help.

To configure log settings for the servers in a site

1. In the console, click **Admin**.
2. On the lower left, click **Servers**.
3. Select the site you want to configure.
4. Under **Tasks**, click **Edit Site Properties**.
5. On the **Log Settings** tab, set the number of entries and number of days to keep log entries for each type of log.

   You can set sizes for management server logs, client logs, and Enforcer logs.
6. Click **OK**.

About configuring event aggregation

You configure event aggregation for client logs in two locations in the Symantec Endpoint Protection Manager console.

Table 22-1 describes where to configure client event aggregation and what the settings mean.

Table 22-1 Client event aggregation

Location	Description
On the **Policies** page, **Antivirus and Antispyware policy**, **Miscellaneous**, **Log Handling** tab	Use this location to configure the aggregation for risk events. The default aggregation time is 5 minutes. The first occurrence of an event is immediately logged. Subsequent occurrences of the same events are aggregated and the number of occurrences is logged on the client every 5 minutes.

Table 22-1 Client event aggregation *(continued)*

Location	Description
On the **Clients** page, **Policies** page, **Client Log Settings**	Use this location to configure the aggregation of Network Threat Protection events. Events are held on the clients for the damper period before they are aggregated into a single event and then uploaded to the console. The damper period helps to reduce events to a manageable number. The default damper period setting is Auto (Automatic). The damper idle period determines the amount of time that must pass between log entries before the next occurrence is considered a new entry. The default damper idle is 10 seconds.

See "Setting up log handling parameters in an Antivirus and Antispyware Policy" on page 409.

See "Configuring client log settings" on page 361.

Configuring client log settings

If you have installed Symantec Endpoint Protection, you can configure some client log options. You can configure the number of entries kept in the logs and the number of days that each entry is kept on the client.

You can configure settings for the following client logs:

- **Control**
- **Packet**
- **Risk**
- **Security**
- **System**
- **Traffic**

lf you have Symantec Network Access Control installed, you can enable and disable logging, and send **Enforcer** logs to the management server. You can also configure the number of log entries and the number of days the entries are kept on the client.

For more information about the Enforcer logs, see the *Implementation Guide for Symantec Network Access Control Enforcement*.

For the **Security**, **Risk**, and **Traffic** logs, you can also configure the damper period and the damper idle period to be used for event aggregation.

You can configure whether or not to upload each type of client log to the server, and the maximum size of the uploads.

If you choose not to upload the client logs, it has the following consequences:

- You cannot view the client log data from the Symantec Endpoint Protection Manager console by using the **Logs** tab on the **Monitoring** page.
- You cannot back up the client logs when you back up the database.
- You cannot export the client log data to a file or a centralized log server.

To configure client log settings

1. On the console, click **Clients**.
2. On the **Policies** tab, under **Location-independent Policies and Settings**, under **Settings**, click **Client Log Settings**.
3. In the **Client Log Settings** for *group name* dialog box, set the maximum file size and the number of days to keep log entries.
4. Check **Upload to management server** for any logs that you want the clients to forward to the server.
5. For the **Security** log and **Traffic** log, set the damper period and the damper idle period.

   These settings determine how frequently **Network Threat Protection** events are aggregated.
6. Set the maximum number of entries that you want a client to upload to the manager at a time.
7. Click **OK**.

About configuring client log handling options for antivirus and antispyware policies

You can configure the following log handling options for antivirus and antispyware policies:

- Which antivirus and antispyware events are forwarded from clients to the Antivirus and Antispyware Protection logs on the server
- How long the events in the Antivirus and Antispyware Protection logs are retained on the server
- How frequently aggregated events are uploaded from clients to the server

See "Setting up log handling parameters in an Antivirus and Antispyware Policy" on page 409.

Backing up the logs for a site

Log data is not backed up unless you configure Symantec Endpoint Protection to back it up. If you do not back up the logs, then only your log configuration options are saved during a backup. You can use the backup to restore your database, but the logs in the database are empty of data when they are restored.

This configuration option is located with the other backup options for local sites on the **Servers** page of the **Admin** page. You can choose to keep up to ten versions of site backups. You should ensure that you have adequate disk space to keep all your data if you choose to keep multiple versions.

To back up the logs for a site

1. On the console, click **Admin**.
2. Select a database server.
3. Under **Tasks**, click **Edit Backup Settings**.
4. In the **Backup Settings** group box, check **Back up logs**.
5. Click **OK**.

About uploading large amounts of client log data

If you have a large number of clients, you may have a large volume of client log data.

You should consider whether or not you want to reduce the volume of data by using the following configurations:

- Upload only some of the client logs to the server.
  See "Configuring client log settings" on page 361.
- Filter the less important risk events and system events out so that less data is forwarded to the server.
  See "Setting up log handling parameters in an Antivirus and Antispyware Policy" on page 409.

If you still plan to upload very large amounts of client log data to a server, you need to consider the following factors:

- The number of clients in your network
- The heartbeat frequency, which controls how often the client logs are uploaded to the server
- The amount of space in the directory where the log data is stored before being inserted into the database

A configuration that uploads a large volume of client log data to the server at frequent intervals can cause space problems. If you must upload a large volume of client log data, you may have to adjust some default values to avoid these space problems. As you deploy to clients, you should monitor the space on the server in the log insertion directory and adjust these values as needed. The default directory where the logs are converted to .dat files and then written into the database is *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\inbox\log. The location of the server data directory is set during installation when you are asked to select the server data folder. You can run the **Management Server Configuration Wizard** from the **Start** menu to change this directory if desired. The \inbox\log directory is automatically added to the directory you set.

The frequency with which the client logs are uploaded is configured on the Policies page of the Clients page, under Communications Settings. The default frequency is to upload the logs every five minutes.

To adjust the values that control the space available on the server, you must change these values in the Windows registry. The Windows registry keys that you need to change are located on the server in HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM.

Table 22-2 lists the Windows registry keys and their default values and describes what they do.

Table 22-2 Windows registry keys that contain log upload settings

Value name	Default and description
MaxInboxSpace	MaxInboxSpace specifies the space that is allotted for the directory where log files are converted to .dat files before they are stored in the database. The default value is 200 MB.
MinDataFreeSpace	MinDataFreeSpace specifies the minimum amount of space that should be kept free in this directory. This key is useful to ensure that other applications that use the same directory have enough space to run without an adverse effect on performance. The default value is 0.
IntervalOfInboxSpaceChecking	IntervalOfInboxSpaceChecking specifies how long Symantec Endpoint Protection waits between checks on the amount of space in the inbox that is available for log data. The default value is 30 seconds.

About managing log events in the database

The database receives and stores a constant flow of entries into its log files. You must manage the data that are stored in the database so that the stored data does not consume all the available disk space. Too much data can cause the computer on which the database runs to crash.

You should understand your default database maintenance settings and change them if the disk space that the database uses seems to grow constantly. If there is a large spike in risk activity, you may need to delete some data to protect the available disk space on the server.

Configuring database maintenance options for logs

Administrators can configure database maintenance options for the data that are stored in the logs. Database maintenance options help you to manage the size of your database by specifying compression settings and how long to keep data.

For information about the specific database maintenance options, refer to the context-sensitive help on the **Site Properties for *site name*** dialog box on the **Database** tab.

To configure database maintenance options for logs

1. On the console, click **Admin**.
2. Select a site.
3. Under **Tasks**, click **Edit Site Properties**.
4. On the **Database** tab, set the number of days to keep risk events.

   To retain the subset of risk infection events after the threshold that you set for risk events, check the **Do not delete infection events** check box.
5. Set how frequently you want to compress identical risk found events into a single event.
6. Set the number of days to keep the events that have been compressed.

   This value includes the time before the events were compressed. For example, suppose that you specify to delete compressed events after ten days and specify to compress events after seven days. In this case, the events are deleted three days after they are compressed.
7. Set the number of days to keep acknowledged and unacknowledged notifications.
8. Set the number of days to keep scan events.

9 Set the number of days to keep the commands that you have run from the console and their associated command status information. After this time, Symantec Endpoint Protection can no longer distribute the commands to their intended recipients.

10 Check the check boxes if you want to delete unused virus definitions and the virus events that contain EICAR as the name of the virus.

The EICAR test virus is a text file that the European Institute for Computer Anti-Virus Research (EICAR) developed. It provides a safe way to test most antivirus software. You can download it from the EICAR Web site. You can use it to verify that the antivirus portion of Symantec Endpoint Protection works.

11 Click **OK**.

About using the Interactive SQL utility with the embedded database

If you choose to use the embedded database with Symantec Endpoint Protection or Symantec Network Access Control, you should note the following information. When you run the database application named Interactive SQL (dbisqlc.exe), it blocks the insertion of data into the embedded database. If you use the application for a while, .dat files accumulate in the *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\inbox\log directories. To alleviate the buildup of the .dat files and restart data insertion into the database, close the application.

Changing timeout parameters

If database errors occur when you view either reports or logs that contain a lot of data, you can make the following changes:

- Change the Microsoft SQL Server connection timeout
- Change the Microsoft SQL Server command timeout

The reporting defaults for these values are as follows:

- Connection timeout is 300 seconds (5 minutes)
- Command timeout is 300 seconds (5 minutes)

If you get CGI or terminated process errors, you might want to change other timeout parameters. See the Symantec Knowledge Base article called "Reporting server does not report or shows a timeout error message when querying large amounts of data."

To change timeout parameters

1. Open the Reporter.php file, which is located in the \Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\Reporting\Resources directory.
2. Use any text editor to add the following settings to the file:
   - **$CommandTimeout =*xxxx***
   - **$ConnectionTimeout =*xxxx***
     Timeout values are in seconds. If you specify zero, or leave the fields blank, the default settings are used.

About recovering a corrupted client System Log on 64-bit computers

If the **System** log becomes corrupted on a 64-bit client, you may see an unspecified error message in the **System** logs on the Symantec Endpoint Protection Manager console. If corrupted, you cannot view the data in the log on the client and the data does not upload to the console. This condition can affect data in the console **Computer Status**, **Risk**, and **Scan** logs and reports.

To correct this condition, you can delete the corrupted log file and the serialize.dat file on the client. These files are located on the client in Drive:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs*date*.Log. After you delete these files, the log file is recreated and begins to log entries correctly.

Chapter 23

Replicating data

This chapter includes the following topics:

About the replication of data

Replication is the process of sharing information between databases to ensure that the content is consistent. You can use replication to increase the number of database servers that are available to clients and thereby reduce the load on each. Replication is typically set up during the initial installation.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for more information on how to set up data replication during an initial installation.

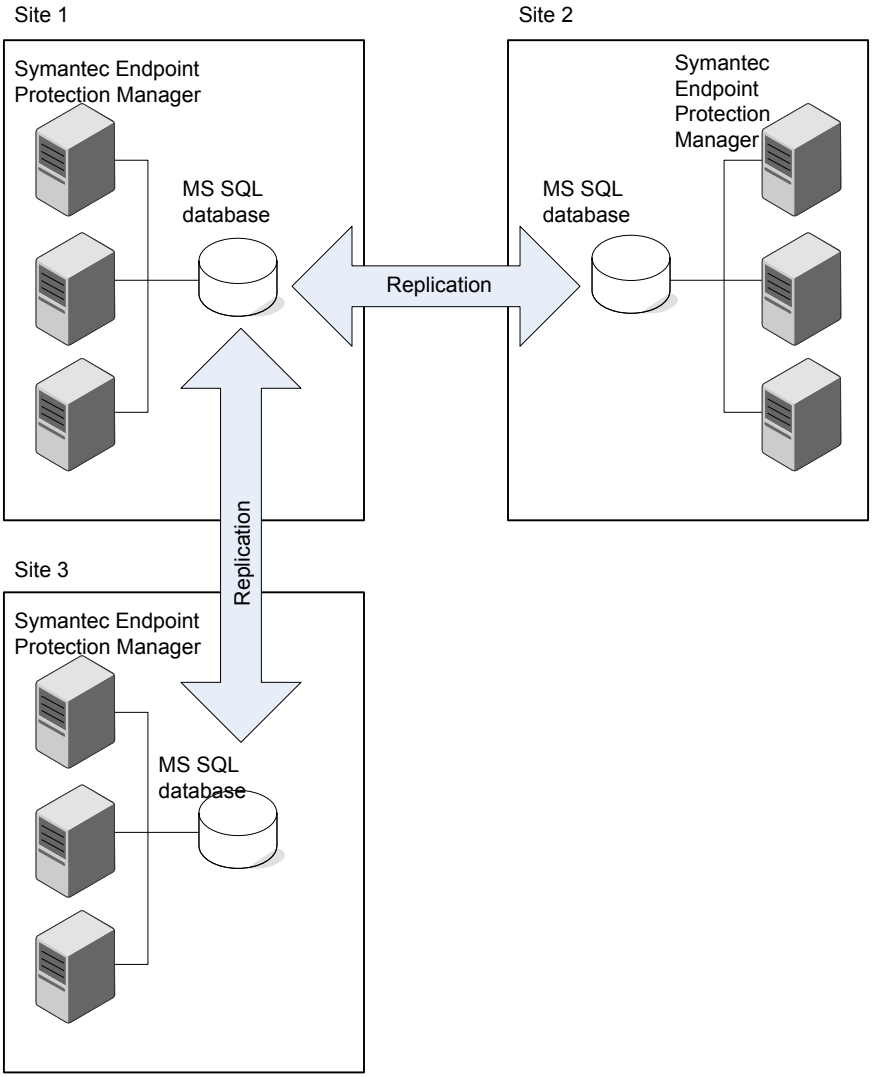
A replication partner is another site with one database server. It also has a connection to the site that you designate as a main site or a local site. A site may have as many replication partners as needed. All replication partners share a common license key. The changes that you made on any replication partner are duplicated to all other replication partners whenever Symantec Endpoint Protection Manager is scheduled to replicate data.

For example, you may want to set up one site at your main office (site 1) and a second site (site 2). Site 2 is a replication partner to the first site. The databases

on site 1 and site 2 are reconciled by using a synchronization schedule that you must set up. If a change is made on site 1, it automatically appears on site 2 after replication occurs. If a change is made on site 2, it automatically appears on site 1 after replication occurs. You can also install a third site (site 3) that can replicate data from either site 1 or site 2. The third site is a replication partner to the other two sites.

Figure 23-1 illustrates how replication of data occurs from a local site to two other sites.

Figure 23-1 An overview of data replication between a local site and two partners



Replication partners are listed on the Admin page. You can display information about replication partners by selecting the partner in the tree. All sites typically have the same type of database. You can, however, set up replication between sites by using different types of databases. In addition, you can also set up replication between an embedded database and an MS SQL database.

If you use an embedded database, you can only connect one Symantec Endpoint Protection Manager to it because of configuration requirements. If you use an MS SQL database, you can connect multiple management servers or share one database. Only the first management server needs to be set up as a replication partner.

All sites that are set up as replication partners are considered to be on the same site farm. Initially, you install the first site, then install a second site as a replication partner. A third site can be installed and set up to connect to either of the first two sites. You can add as many sites as needed to the site farm.

You can delete replication partners to stop the replication. Later you can add that replication partner back to make the databases consistent. However, some changes may collide.

See "About the settings that are replicated" on page 372.

You can set up data replication during the initial installation or at a later time. When you set up replication during the initial installation, you can also set up a schedule for the synchronization of the replication partners.

About the impact of replication

If administrators make changes on at each replication site simultaneously, some changes may get lost. If you change the same setting on both sites and a conflict arises, the last change is the one that takes effect when replication occurs.

For example, site 1 (New York) replicates with site 2 (Tokyo) and site 2 replicates with site 3 (London). You want the clients that connect to the network in New York to also connect with the Symantec Endpoint Protection Manager in New York. However, you do not want them to connect to the management server in either Tokyo or London.

About the settings that are replicated

When you set up replication, client communication settings are also replicated. Therefore, you need to make sure that the communication settings are correct for all sites on the site farm in the following manner:

- Create generic communication settings so that a client's connection is based on the type of connection. For example, you can use a generic DNS name, such as symantec.com for all sites on a site farm. Whenever clients connect, the DNS server resolves the name and connects the client to the local Symantec Endpoint Protection Manager.
- Create specific communication settings by assigning groups to sites so that all clients in a group connect to a designated management server.

For example, you can create two groups for clients at site 1, two different groups for site 2, and two other groups for site 3. You can apply the communication settings at the group level so clients connect to the designated management server.

You may want to set up guidelines for managing location settings for groups. Guidelines may help prevent conflicts from occurring on the same locations. You may also help prevent conflicts from occurring for any groups that are located at different sites.

How changes are merged during replication

After replication occurs, the database on site 1 and the database on site 2 are the same. Only computer identification information for the servers differs.

If administrators change settings on all sites on a site farm, conflicts can occur. For example, administrators on site 1 and site 2 can both add a group with the same name. If you want to resolve this conflict, both groups then exist after replication. However, one of them is renamed with a tilde and the numeral 1 (~1).

If both sites added a group that is called Sales, after replication you can see two groups at both sites. One group is called Sales and the other is called Sales 1. This duplication occurs whenever a policy with the same name is added to the same place at two sites.

If duplicate network adapters are created at different sites with the same name, a tilde and the numeral 1 (~1) is added. The two symbols are added to one of the names.

If different settings are changed at both sites, the changes are merged after replication. For example, if you change Client Security Settings on site 1 and Password Protection on site 2, both sets of changes appear after replication. Whenever possible, changes are merged between the two sites.

If policies are added at both sites, new policies appear on both sites after replication. Conflicts can occur when one policy is changed at two different sites. If a policy is changed at multiple sites, the last update of any change is then maintained after replication.

If you perform the following tasks with the replication that is scheduled to occur every hour on the hour:

- You edit the AvAsPolicy1 on site 1 at 2:00 P.M.
- You edit the same policy on site 2 at 2:30 P.M.

Then only the changes that have been completed on site 2 appear after replication is complete when replication occurs at 3:00 P.M.

If one of the replication partners is taken offline, the remote site may still indicate the status as online.

Adding and disconnecting a replication partner

If you want to replicate data with another site, you may have already set it up during the initial installation. If you did not set up replication during the initial installation, you can do so now by adding a replication partner. Multiple sites are called a site farm whenever they are set up as replication partners. You can add any site on the site farm as a replication partner.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for more information.

Also, you can add a replication partner that was previously deleted as a partner.

Before you begin, you need to have the following information:

- An IP address or host name of the Symantec Endpoint Protection Manager for which you want to make a replication partner.
- The management server to which you want to connect must have previously been a replication partner. The management server can have also been a partner to another site on the same site farm.

To add a replication partner

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, select a site.
3. Under Tasks, click **Add Replication Partner**.
4. In the Add Replication Partner wizard, click **Next**.
5. Type the IP address or host name of the management server that you want to make a replication partner.
6. Type the port number of the remote server on which you installed the management server.

   The default setting for the remote server port is 8443.
7. Type the administrator's user name and password.
8. Click **Next**.
9. In the Schedule Replication pane, specify the schedule for replication between the two partners by doing one of the following:
   - Check **Autoreplicate**.

It causes frequent and automatic replication to occur between two sites. This option is the default setting. Therefore you cannot set up a custom schedule for replication.

- Uncheck **Autoreplicate**
  You can now set up a custom schedule for replication:
  - Select the hourly, daily, or weekly **Replication Frequency**.
  - Select the specific day during which you want replication to occur in the **Day of Week** list to set up a weekly schedule.

10 Click **Next**.

11 In the Replication of Log Files and Client Packages pane, check or uncheck the options depending on whether or not you want to replicate logs.

The default setting is unchecked.

12 On the Add Replication Partner dialog do one of the following:

- If the database has been restored on the replication partner site, click **Yes**. You must restore the database on each replication partner site before you continue if you are upgrading or restoring a database.
- Click **No** if the database has not been restored. Then restore the database and restart this procedure.

13 Click **Next**.

14 Click **Finish**.

The replication partner site is added under Replication Partners on the Admin page.

Disconnecting replication partners

Deleting a replication partner merely disconnects a replication partner from Symantec Endpoint Protection Manager. It does not delete the site. You can add the site back later if you need to do so by adding a replication partner.

To remove databases from the replication process

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

2 In the Admin page, under View Servers, click **Replication Partners**.

3 Expand **Replication Partners** and select the partner from which you want to disconnect.

4 In the Admin page, under asks pane, click **Delete Replication Partner**.

5 Type **Yes** when asked to verify that you want to delete the replication partner.

Scheduling automatic and on-demand replication

You can schedule replication automatically or on demand. You can also specify the frequency with which you want to schedule replication.

Replicating data on demand

Replication normally occurs according to the schedule that you set up when you added a replication partner during installation. The site with the smaller ID number initiates the scheduled replication. At times, you may want replication to occur immediately.

Scheduling on-demand replication

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, expand **Replication Partners** and select the partner whose database you want to replicate immediately.
3. Under Tasks, click **Replicate Now**.
4. Click **Yes** when asked to verify that you want to start a one time replication now.

   The following message appears:

   ```
   Replication has been scheduled.
   For details regarding the  outcome of the scheduled
   event,  please check the server system logs after
   a few minutes delay. The delay depends on the load
   of the server, the amount of changes to be replicated,
   and the bandwidth of the communication channel.
   ```

5. Click **OK**. The database is replicated immediately.

   If you use a Microsoft SQL database with more than one server, you can only initiate replication from the first server at that site. If you try to replicate now from the second server, the following message appears:

   ```
   Only the first server of the site can perform the replication.
   Please log on to the server: <first server name> to start
   replication.
   ```

Changing replication frequencies

Replication normally occurs according to the schedule that you set up when you added a replication partner during the initial installation. The site with the smaller

ID number initiates the scheduled replication. When a replication partner has been established, you can change the replication schedule. When you change the schedule on a replication partner, the schedule on both sides is the same after the next replication.

To change replication frequencies

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, click **Replication Partners**.
3. Under Tasks, click **Edit Replication Partner**.
4. In the Edit Replication Partner dialog box, specify the schedule for replication between the two partners by doing one of the following:
   - Check **Autoreplicate**.
     It causes frequent and automatic replication to occur between two sites. This option is the default setting. Therefore you cannot set up a custom schedule for replication.
   - Uncheck **Autoreplicate**
     You can now set up a custom schedule for replication.
     - Select the hourly, daily, or weekly **Replication Frequency**.
     - Select the specific day during which you want replication to occur in the **Day of Week** list to set up a weekly schedule.
5. Click **OK**.

Replicating client packages and LiveUpdate content

You can replicate or duplicate client packages and LiveUpdate content between the local site and this partner at a remote site. You may want to copy the latest version of a client package or LiveUpdate content from a local site to a remote site. The administrator at the remote site can then deploy the client package and LiveUpdate content.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for more information on how to create and deploy client installation packages at a site.

If you decide to replicate client packages and LiveUpdate content, you may duplicate a large volume of data. Should you replicate many packages, the data may be as large as 5 GB. Both Symantec Endpoint Protection and Symantec Network Access Control 32- bit and 64-bit installation packages may require as much as 500 MB of disk space.

See the *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* for more information about requirements for disk storage.

To replicate client packages and LiveUpdate content

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, click **Replications Partners**.
3. Expand **Replication Partners** and select the replication partner with which you want to replicate client packages.
4. Under Tasks, click **Edit Replication Partner Properties**.
5. In the Replication Partner Properties dialog box, under Partner, click **Replicate client packages between local site and partner site**.
6. Click **OK**.

Replicating logs

You can specify that you want to replicate or duplicate logs as well as the database of a replication partner. You can specify the replication of logs when adding replication partners or by editing the replication partner properties. If you plan to replicate logs, make sure that you have sufficient disk space for the additional logs on all the replication partner computers.

See "Viewing logs from other sites" on page 269.

To replicate logs between replication partners

1. In the console, click **Admin**, and then click **Servers**.
2. Under View Servers, click **Replications Partners**.
3. Expand **Replication Partners** and select the replication partner for which you want to start generating replication logs.
4. In the Admin page, under Tasks, click **Edit Replication Partner Properties**.
5. In the Replication Partner Properties dialog box, under Partner, click **Replicate logs from local site to this partner site** or **Replicate logs from this partner site to local site**.
6. Click **OK**.

Chapter 24

Managing Tamper Protection

This chapter includes the following topics:

About Tamper Protection

Tamper Protection provides real-time protection for Symantec applications that run on servers and clients. It prevents non-Symantec processes such as worms, Trojan horses, viruses, and security risks, from affecting Symantec processes. You can configure the software to block or log attempts to modify Symantec processes.

Note: If you use third-party security risk scanners that detect and defend against unwanted adware and spyware, these scanners typically impact Symantec processes. If you have Tamper Protection enabled when you run such a scanner, Tamper Protection generates a large number of notifications and log entries. A best practice for Tamper Protection is to always leave it enabled. Use log filtering if the number of the events generated is too large.

When a client is installed as an unmanaged client, Tamper Protection has the following default values:

- Tamper Protection is enabled.
- The action that Tamper Protection takes when it detects a tamper attempt is to block the attempt and log the event.

- Tamper Protection sends the user a default message when it detects a tamper attempt.

You can turn off Tamper Protection notifications on client computers. You can also create exceptions for applications that Tamper Protection detects.

See "Configuring Tamper Protection" on page 380.

See "Configuring a centralized exception for Tamper Protection" on page 585.

See "Adding a centralized exception for Tamper Protection events" on page 588.

When a client is installed as a managed client, Tamper Protection has the following default values:

- Tamper Protection is enabled.
- The action that Tamper Protection takes when it detects a tamper attempt is to log the event only.
- Tamper Protection does not send the user a message when it detects a tamper attempt.

Note: If you enable notifications when Symantec Endpoint Protection detects a tamper attempt, notifications about Windows processes are sent to affected computers as well as notifications about Symantec processes.

See "Configuring Tamper Protection" on page 380.

Configuring Tamper Protection

You can enable and disable Tamper Protection and configure the action that it takes when it detects a tampering attempt. You can also configure it to notify users when it detects a tampering attempt.

A best practice when you initially use Symantec Endpoint Protection is to use the action **Log the event only** while you monitor the logs once a week. When you are comfortable that you see no false positives, then set Tamper Protection to **Block it and log the event**.

See "About Tamper Protection" on page 379.

You can configure a message to appear on clients when Symantec Endpoint Protection detects a tamper attempt. By default, notification messages appear when the software detects a tamper attempt.

The message that you create can contain a mix of text and variables. The variables are populated with the values that identify characteristics of the attack. If you use a variable, you must type it exactly as it appears.

Table 24-1 describes the variables you can use to configure a message.

Table 24-1 Tamper Protection message variables and descriptions

Field	Description
[ActionTaken]	The action that Tamper Protection performed to respond to the attack.
[ActorProcessID]	The ID number of the process that attacked a Symantec application.
[ActorProcessName]	The name of the process that attacked a Symantec application.
[Computer]	The name of the computer that was attacked.
[DateFound]	The date on which the attack occurred.
[EntityType]	The type of target that the process attacked.
[Filename]	The name of the file that attacked the protected processes.
[Location]	The area of the computer hardware or software that was protected from tampering. For Tamper Protection messages, this field is Symantec applications.
[PathAndFilename]	The complete path and name of the file that attacked protected processes.
[SystemEvent]	The type of the tamper attempt that occurred.
[TargetPathname]	The location of the target that the process attacked.
[TargetProcessID]	The process ID of the target that the process attacked.
[TargetTerminalSession ID]	The ID of the terminal session during which the event occurred.
[User]	The name of the logged on user when the attack occurred.

To enable or disable Tamper Protection

1. In the console, click **Clients**.
2. On the Policies tab, under Settings, click **General Settings**.
3. On the Tamper Protection tab, check or uncheck **Protect Symantec security software from being tampered with or shut down**.
4. Click the lock icon if you do not want users to be able to change this setting.
5. Click **OK**.

To configure basic Tamper Protection settings

1. In the console, click **Clients**.
2. On the Policies tab, under Settings, click **General Settings**.
3. On the Tamper Protection tab, in the list box, select one of the following actions:
   - To block and log unauthorized activity, click **Block it and log the event**.
   - To log unauthorized activity but allow the activity to take place, click **Log the event only**.
4. Click the lock icon if you do not want users to be able to change this setting.
5. Click **OK**.

To enable and customize Tamper Protection notification messages

1. In the console, click **Clients**.
2. On the Policies tab, under Settings, click **General Settings**.
3. On the Tamper Protection tab, click **Display a notification message when tampering is detected**.
4. In the text field box, if you want to modify the default message, you can type additional text and delete text.

   If you use a variable, you must type it exactly as it appears.
5. Click the lock icon if you do not want users to be able to change this setting.
6. Click **OK**.

Section 3

Configuring Antivirus and Antispyware Protection

Chapter 25

Basic Antivirus and Antispyware Policy settings

This chapter includes the following topics:

- Managing quarantined files

Basics of Antivirus and Antispyware Protection

You can provide Antivirus and Antispyware Protection for computers in your security network by doing the following actions:

- Create a plan to respond to viruses and security risks.
  See "About creating a plan to respond to viruses and security risks" on page 386.
- View the status of your network on the Home page in the console.
  See "About the Symantec Endpoint Protection Home page" on page 198.
- Run commands from the console to turn on Auto-Protect, launch an on-demand scan, or update definitions.
  See "Running commands on clients from the console" on page 76.
  See "Running on-demand scans" on page 453.
  See "Managing content for clients" on page 132.
- Use Antivirus and Antispyware Policies to modify Auto-Protect and scan settings on client computers.
  See "Configuring File System Auto-Protect for Windows clients" on page 431.
  See "Configuring advanced scanning and monitoring options" on page 433.

About creating a plan to respond to viruses and security risks

An effective response to a virus and security risk outbreak requires a plan that lets you respond quickly and efficiently. You should create an outbreak plan and define actions to handle suspicious files.

See "Basics of Antivirus and Antispyware Protection" on page 386.

Table 25-1 outlines the tasks for creating a virus and security risk outbreak plan.

Table 25-1 A sample plan

Task	Description
Ensure that definitions files are current.	Verify that infected computers have the latest definitions files. You can run reports to check that client computers have the latest definitions. To update definitions, do any of the following actions: ■ Apply a LiveUpdate policy. See "About LiveUpdate Policies" on page 142. ■ Run the Update Content command for a group or the selected computers that are listed on the Clients tab. ■ Run the Update Content command on the selected computers that are listed in a computer status or risk log.
Map your network topology.	Prepare a network topology map so that you can systematically isolate and clean computers by segment before you reconnect them to your local network. Your map should contain the following information: ■ Client computer names and addresses ■ Network protocols ■ Shared resources
Understand security solutions.	You should understand your network topology and your implementation of the client in your network. You should also understand the implementation of any other security products that are used on your network. Consider the following questions: ■ What security programs protect network servers and workstations? ■ What is the schedule for updating definitions? ■ What alternative methods to obtain updates are available if the normal channels are under attack? ■ What log files are available to track viruses on your network?
Have a backup plan.	In the event of a catastrophic infection, you may need to restore client computers. Make sure that you have a backup plan in place to restore critical computers.

Table 25-1 A sample plan *(continued)*

Task	Description
Isolate the infected computers.	Blended threats such as worms can travel by shared resources without user interaction. When you respond to an infection by a computer worm, it can be critical to isolate the infected computers by disconnecting them from the network.
Identify the risk.	The management console reports and logs are a good source of information about risks on your network. You can use the Symantec Security Response Virus Encyclopedia to learn more about a particular risk that you identify in reports or logs. In some cases, you might find additional instructions for handling the risk.
Respond to unknown risks.	You should look at the Symantec Security Response Web site for up-to-date information when the following situations are true: ■ You cannot identify a suspicious file by examining the logs and reports. ■ The latest virus definitions files do not clean the suspicious file. On the Web site, you might find recent information about the suspicious file. Check the Latest Virus Threats and Security Advisories. http://securityresponse.symantec.com

About Symantec Security Response

You can check the Symantec Security Response Web pages for up-to-date information about viruses and security risks.

http://securityresponse.symantec.com

http://www.symantec.com/enterprise/security_response/

About viewing the antivirus and antispyware status of your network

You can quickly view the status of your security network on the Home page in the console. A status summary shows you how many computers in your security network have disabled Antivirus and Antispyware Protection. An action summary shows the actions that the client performed on the detected viruses and security risks. The Home page also includes the virus definitions distribution across the network.

See "About the Symantec Endpoint Protection Home page" on page 198.

You can also run reports and view logs.

See "Monitoring endpoint protection" on page 191.

About running commands for Antivirus and Antispyware Protection

You can quickly run commands from the Clients page in the console or by using the computer status logs from the Monitors page.

See "Running commands on clients from the console" on page 76.

See "Running commands and actions from logs" on page 274.

About enabling Auto-Protect manually

The default Antivirus and Antispyware Policy enables Auto-Protect by default. If users on client computers disable Auto-Protect, you can quickly re-enable it in the console.

You can select the computers for which you want to enable Auto-Protect in the console on the Clients page. You can also enable Auto-Protect from a log that you generate from the Monitors page.

See "Enabling File System Auto-Protect" on page 430.

About running on-demand scans

You can include scheduled scans as part of Antivirus and Antispyware Policies. However, you might need to manually run scans on client computers.

You can select computers for which you want to run on-demand scans in the console on the Clients page. You can also run an on-demand scan from a log that you generate from the Monitors page.

You can run an active, full, or custom scan. If you choose to run a custom scan, the client uses the settings for on-demand scans that you configure in the Antivirus and Antispyware Policy.

See "Running on-demand scans" on page 453.

About Antivirus and Antispyware Policies

An Antivirus and Antispyware Policy includes the following types of options:

- Auto-Protect scans
- Administrator-defined scans (scheduled and on-demand scans)

- TruScan proactive threat scans
- Quarantine options
- Submissions options
- Miscellaneous parameters

When you install Symantec Endpoint Protection, several Antivirus and Antispyware Policies appears in the policy list in the console. You can modify one of the preconfigured policies, or you can create new policies.

Note: Antivirus and Antispyware Policies include configuration for TruScan proactive threat scans.

See "About scanning" on page 396.

About the preconfigured Antivirus and Antispyware Policies

The following preconfigured Antivirus and Antispyware Policies are available:

- Antivirus and Antispyware Policy
- Antivirus and Antispyware Policy - High Security
- Antivirus and Antispyware Policy - High Performance

The High Security Policy is the most stringent of all the preconfigured Antivirus and Antispyware Policies. You should be aware that it can affect the performance of other applications.

The High Performance Policy provides better performance than the High Security Policy, but it does not provide the same safeguards. It relies primarily on File System Auto-Protect to scan files with selected file extensions to detect threats.

The default Antivirus and Antispyware Policy contains the following important settings:

- File System Auto-Protect loads at computer startup and is enabled for all files.
- Internet Email, Microsoft Outlook, and Lotus Notes Auto-Protect are enabled for all files.
- File System Auto-Protect network scanning is enabled.
- TruScan proactive threat scans are enabled, and run once every hour.
- ActiveScan does not run automatically when new definitions arrive.
- A scheduled scan runs once per week, with scan tuning set to Best Application Performance.

The High Performance Policy contains the following important settings:

- File System Auto-Protect loads when Symantec Endpoint Protection starts and is enabled for files with selected extensions.
- File System Auto-Protect network scanning is disabled.
- Internet Email, Microsoft Outlook, and Lotus Notes Auto-Protect are disabled.
- Proactive threat scans are enabled, and run once every 6 hours.
- ActiveScan does not run automatically when new definitions arrive.
- A scheduled scan runs once a month with scan tuning set to Best Application Performance.

The High Security Policy contains the following important settings:

- File System Auto-Protect loads at computer startup and is enabled for all files.
- Internet Email, Microsoft Outlook, and Lotus Notes Auto-Protect are enabled for all files.
- File System Auto-Protect network scanning is enabled.
- Proactive threat scans are enabled and run once every hour, as well as every time a new process starts.
- ActiveScan runs automatically when new definitions arrive.
- A scheduled scan runs once per week, with scan tuning set to Balanced.

About locking settings in Antivirus and Antispyware Policies

You can lock some settings in an Antivirus and Antispyware Policy. When you lock settings, users cannot change the settings on the client computers that use the policy.

About Antivirus and Antispyware Policies for legacy clients

If your environment contains multiple versions of legacy clients, your Antivirus and Antispyware Policy might contain the settings that cannot be applied. You might need to configure and manage separate Antivirus and Antispyware Policies for legacy clients.

About default settings for handling suspicious files

Using the default Antivirus and Antispyware Policy, the Symantec Endpoint Protection client performs the following actions when it identifies a file that it suspects a virus infected:

- The client tries to repair the file.
- If the file cannot be repaired with the current set of definitions, the client moves the infected file to the local Quarantine. In addition, the client makes a log entry of the risk event. The client forwards the data to the management server. You can view the log data from the console.

You can perform the following additional actions to complete your virus handling strategy:

- Configure the reports feature to notify you when viruses are found.
  See "About using notifications" on page 281.
- Define the different repair actions that are based on the virus type. For example, you can configure the client to fix macro viruses automatically. Then you can configure a different action for the client to take when it detects a program file.
- Assign a backup action for the files that the client cannot repair.

  See "Configuring actions for known virus and security risk detections on Windows clients" on page 417.
- Configure the local Quarantine to forward infected files to a Central Quarantine Server. You can configure the Central Quarantine to try a repair. When the Central Quarantine tries a repair, it uses its set of virus definitions. The Central Quarantine definitions might be more up to date than the definitions on the local computer. You can also automatically forward samples of infected files to Symantec Security Response for analysis.

  For more information, see the *Symantec Central Quarantine Implementation Guide*.

About using policies to manage items in the Quarantine

When the client detects a known virus, it places the file in the client computer's local Quarantine. The client might also quarantine the items that proactive threat scans detect. You configure the Quarantine settings as part of an Antivirus and Antispyware Policy that you apply to clients.

You can specify the following:

- A local Quarantine directory path
- Whether clients manually submit quarantined items to Symantec Security Response
- Whether clients automatically submit quarantined items to a Central Quarantine Server

- How the local Quarantine handles remediation when new virus definitions arrive

See "Managing quarantined files" on page 424.

You can also delete quarantined items on your client computers from the Risk log in the console.

See "Monitoring endpoint protection" on page 191.

About working with Antivirus and Antispyware Policies

You create and edit Antivirus and Antispyware Policies similarly to how you create and modify other types of policies. You can assign, withdraw, replace, copy, export, import, or delete an Antivirus and Antispyware Policy.

You typically assign a policy to multiple groups in your security network. You can create a non-shared, location-specific policy if you have specific requirements for a particular location.

The procedures in this chapter assume that you are familiar with the basics of policy configuration.

See "Using policies to manage your network security" on page 90.

About viruses and security risks

An Antivirus and Antispyware Policy scans for both viruses and for security risks; examples of security risks are spyware, adware, and other files that can put a computer or a network at risk. Antivirus and antispyware scans detect kernel-level rootkits. Rootkits are the programs that try to hide themselves from a computer's operating system and can be used for malicious purposes.

The default Antivirus and Antispyware Policy does the following actions:

- Detects, removes, and repairs the side effects of viruses, worms, Trojan horses, and blended threats.
- Detects, removes, and repairs the side effects of security risks such as adware, dialers, hacking tools, joke programs, remote access programs, spyware, trackware, and others.

See "Basics of Antivirus and Antispyware Protection" on page 386.

Table 25-2 describes the types of risks for which the client software scans.

Table 25-2 Viruses and security risks

Risk	Description
Viruses	Programs or code that attach a copy of themselves to another computer program or document when it runs. When the infected program runs, the attached virus program activates and attaches itself to other programs and documents. When a user opens a document that contains a macro virus, the attached virus program activates and attaches itself to other programs and documents. Viruses generally deliver a payload, such as displaying a message on a particular date. Some viruses specifically damage data. These viruses can corrupt programs, delete files, or reformat disks.
Malicious Internet bots	Programs that run automated tasks over the Internet for malicious purposes. Bots can be used to automate attacks on computers or to collect information from Web sites.
Worms	Programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down.
Trojan horses	Malicious programs that hide themselves in something benign, such as a game or utility.
Blended threats	Threats that blend the characteristics of viruses, worms, Trojan horses, and code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. Blended threats use multiple methods and techniques to spread rapidly and cause widespread damage throughout the network.
Adware	Stand-alone or appended programs that secretly gather personal information through the Internet and relay it back to another computer. Adware may track browsing habits for advertising purposes. Adware can also deliver advertising content. Adware can be unknowingly downloaded from Web sites, typically in shareware or freeware, or can arrive through email messages or instant messenger programs. Often a user unknowingly downloads adware by accepting an End User License Agreement from a software program.
Dialers	Programs that use a computer, without the user's permission or knowledge, to dial out through the Internet to a 900 number or FTP site. Typically, these numbers are dialed to accrue charges.

Table 25-2 Viruses and security risks *(continued)*

Risk	Description
Hacking tools	Programs that are used by a hacker to gain unauthorized access to a user's computer. For example, one hacking tool is a keystroke logger, which tracks and records individual keystrokes and sends this information back to the hacker. The hacker can then perform port scans or vulnerability scans. Hacking tools may also be used to create viruses.
Joke programs	Programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or frightening. For example, a program can be downloaded from a Web site, email message, or instant messenger program. It can move the Recycle Bin away from the mouse when the user tries to delete it or cause the mouse to click in reverse.
Other	Other security risks that do not conform to the strict definitions of viruses, Trojan horses, worms, or other security risk categories.
Remote access programs	Programs that allow access over the Internet from another computer so that they can gain information or attack or alter a user's computer. For example, a user may install a program, or another process might install a program without the user's knowledge. The program can be used for malicious purposes with or without modification of the original remote access program.
Spyware	Stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and relay it back to another computer. Spyware can be unknowingly downloaded from Web sites, typically in shareware or freeware, or can arrive through email messages or instant messenger programs. Often a user unknowingly downloads spyware by accepting an End User License Agreement from a software program.
Trackware	Stand-alone or appended applications that trace a user's path on the Internet and send information to the target system. For example, the application can be downloaded from a Web site, email message, or instant messenger program. It can then obtain confidential information regarding user behavior.

By default, Auto-Protect scans for viruses, Trojan horses, worms, and security risks when it runs.

Some risks, such as Back Orifice, were detected as viruses in earlier versions of the client software. They remain detected as viruses so that the client software can continue to provide protection for legacy computers.

About scanning

You can include the following types of scans in an Antivirus and Antispyware Policy:

- Antivirus and antispyware scans
  - Auto-Protect scans
    See "About Auto-Protect scans" on page 396.
  - Administrator-defined scans
    See "About administrator-defined scans" on page 401.
- TruScan proactive threat scans
  See "About TruScan proactive threat scans" on page 402.

By default, all antivirus and antispyware scans detect viruses and security risks, such as adware and spyware; the scans quarantine the viruses and the security risks, and then they remove or repair their side effects. Auto-Protect and administrator-defined scans detect known viruses and security risks. Proactive threat scans detect unknown viruses and security risks by scanning for potentially malicious behavior.

Note: Sometimes, you might unknowingly install an application that includes a security risk such as adware or spyware. If Symantec determines that blocking the risk does not harm the computer, the client software blocks the risk. If blocking the risk might leave the computer in an unstable state, the client waits until the application installation is complete before it quarantines the risk. It then repairs the risk's side effects.

About Auto-Protect scans

Auto-Protect scans include the following types of scans:

- File System Auto-Protect scans
- Auto-Protect email attachment scans for Lotus Notes and Outlook (MAPI and Internet)
- Auto-Protect scans for the Internet email messages and the attachments that use the POP3 or SMTP communications protocols; Auto-Protect scans for Internet email also include outbound email heuristics scanning

Note: For performance reasons, Internet Email Auto-Protect for POP3 is not supported on server operating systems. On a Microsoft Exchange server, you should not install Microsoft Outlook Auto-Protect.

Auto-Protect continuously scans files and email data for viruses and for security risks; viruses and security risks can include spyware and adware, as they are read from or written to a computer.

You can configure Auto-Protect to scan only selected file extensions. When it scans selected extensions, Auto-Protect can also determine a file's type even if a virus changes the file's extension.

When you configure Auto-Protect settings, you can lock Auto-Protect options on clients to enforce a company security policy for viruses and security risks. Users cannot change the options that you lock.

Auto-Protect is enabled by default. You can view Auto-Protect status in the console under the Clients tab or by generating the reports and the logs that show computer status. You can also view Auto-Protect status directly on the client.

Auto-Protect scans can scan email attachments for the following applications:

- Lotus Notes 4.5x, 4.6, 5.0, and 6.x
- Microsoft Outlook 98/2000/2002/2003/2007 (MAPI and Internet)

If you use Microsoft Outlook over MAPI or Microsoft Exchange client and you have Auto-Protect enabled for email, attachments are immediately downloaded to the computer that is running the email client. The attachments are scanned when the user opens the attachment. If you download a large attachment over a slow connection, mail performance is affected. You may want to disable this feature for users who regularly receive large attachments.

Note: If Lotus Notes or Microsoft Outlook is already installed on the computer when you perform a client software installation, the client software detects the email application. The client then installs the correct Auto-Protect email type. Both types are installed if you select a complete installation when you perform a manual installation.

If your email program is not one of the supported data formats, you can protect your network by enabling Auto-Protect on your file system. If a user receives a message with an infected attachment on a Novell GroupWise Email system, Auto-Protect can detect the virus when the user opens the attachment. This outcome is because most email programs save attachments to a temporary directory when users launch attachments from the email program. If you enable Auto-Protect on your file system, Auto-Protect detects the virus as it is written

to the temporary directory. Auto-Protect also detects the virus if the user tries to save the infected attachment to a local drive or network drive.

See "About configuring Auto-Protect" on page 429.

See "About Auto-Protect detection of the processes that continuously download the same security risk" on page 398.

See "About the automatic exclusion of files and folders" on page 398.

See "If client email applications use a single inbox" on page 400.

About Auto-Protect detection of the processes that continuously download the same security risk

If Auto-Protect detects a process that continuously downloads a security risk to a client computer, Auto-Protect can display a notification and log the detection. (Auto-Protect must be configured to send notifications.) If the process continues to download the same security risk, multiple notifications appear on the user's computer, and Auto-Protect logs multiple events. To prevent multiple notifications and logged events, Auto-Protect automatically stops sending notifications about the security risk after three detections. Auto-Protect also stops logging the event after three detections.

In some situations, Auto-Protect does not stop sending notifications and logging events for the security risk.

Auto-Protect continues to send notifications and log events when any of the following is true:

- You or users on client computers disable blocking the installation of security risks (the default is enabled).
- The action for the type of security risk that the process downloads has an action of Leave alone.

About the automatic exclusion of files and folders

The client software automatically detects the presence of certain third-party applications and Symantec products. After it detects them, it creates exclusions for these files and folders. The client excludes these files and folders from all antivirus and antispyware scans.

The client software automatically creates exclusions for the following items:

- Microsoft Exchange
- Active Directory domain controller
- Certain Symantec products

Note: To see the exclusions that the client creates on 32-bit computers, you can examine the contents of the HKEY_LOCAL_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\Exclusions Windows registry. You must not edit this Windows registry directly. On 64-bit computers, look in HKEY_LOCAL_MACHINE\Software\Wow6432Node\Symantec\Symantec Endpoint Protection\AV\Exclusions.

The client does not exclude the system temporary folders from scans because doing so can create a significant security vulnerability on a computer.

You can configure any additional exclusions by using centralized exceptions.

See "Configuring a Centralized Exceptions Policy" on page 579.

About the automatic exclusion of files and folders for Microsoft Exchange server

If Microsoft Exchange servers are installed on the computer where you installed the Symantec Endpoint Protection client, the client software automatically detects the presence of Microsoft Exchange. When the client software detects a Microsoft Exchange server, it creates the appropriate file and folder exclusions for File System Auto-Protect and all other scans. Microsoft Exchange servers can include clustered servers. The client software checks for changes in the location of the appropriate Microsoft Exchange files and folders at regular intervals. If you install Microsoft Exchange on a computer where the client software is already installed, the exclusions are created when the client checks for changes. The client excludes both files and folders; if a single file is moved from an excluded folder, the file remains excluded.

The client software creates file and folder scan exclusions for the following Microsoft Exchange server versions:

- Exchange 5.5
- Exchange 6.0
- Exchange 2000
- Exchange 2003
- Exchange 2007
- Exchange 2007 SP1

For Exchange 2007, see your user documentation for information about compatibility with antivirus software. In a few circumstances, you might need to create scan exclusions for some Exchange 2007 folders manually. For example, in a clustered environment, you might need to create some exclusions.

For more information, see the following document in the Symantec Knowledge Base: Preventing Symantec Endpoint Protection 11.0 from scanning the Microsoft Exchange 2007 directory structure.

About the automatic exclusion of files and folders from Symantec products

The client creates appropriate file and folder scan exclusions for certain Symantec products when they are detected.

The client creates exclusions for the following Symantec products:

- Symantec Mail Security 4.0, 4.5, 4.6, 5.0, and 6.0 for Microsoft Exchange
- Symantec AntiVirus/Filtering 3.0 for Microsoft Exchange
- Norton AntiVirus 2.x for Microsoft Exchange
- Symantec Endpoint Protection Manager embedded database and logs

About the automatic exclusion of Active Directory files and folders

The client software creates file and folder exclusions for the Active Directory domain controller database, logs, and working files. The client monitors the applications that are installed on the client computer. If the software detects Active Directory on the client computer, the software automatically creates the exclusions.

If client email applications use a single inbox

The applications that store all email in a single file include Outlook Express, Eudora, Mozilla, and Netscape. If your client computers use any email applications that use a single inbox, you should create a centralized exception to exclude the Inbox file. The exception applies to all antivirus and antispyware scans as well as Auto-Protect.

The Symantec Endpoint Protection client quarantines the entire Inbox and users cannot access their email if the following statements are true:

- The client detects a virus in the Inbox file during an on-demand or scheduled scan.
- The action that is configured for the virus is Quarantine.

Symantec does not usually recommend excluding files from scans. When you exclude the Inbox file from scans, the Inbox cannot be quarantined; however, if the client detects a virus when a user opens an email message, it can safely quarantine or delete the message.

About administrator-defined scans

Administrator-defined scans are the antivirus and antispyware scans that detect known viruses and security risks. For the most complete protection, you should schedule occasional scans for your client computers. Unlike Auto-Protect, which scans files and email as they are read to and from the computer, administrator-defined scans detect viruses and security risks. Administrator-defined scans detect viruses and security risks by examining all files and processes (or a subset of files and processes). Administrator-defined scans can also scan memory and load points.

You configure administrator-defined scans as part of an Antivirus and Antispyware Policy.

Administrator-defined scans include the following types of scans:

- Scheduled scans
  See "About scheduled scans" on page 401.
- On-demand scans
  See "About on-demand scans" on page 402.

Typically, you might want to create a full scheduled scan to run once a week, and an Active Scan to run once per day. By default, Symantec Endpoint Protection client generates an Active Scan to run at startup on client computers.

About scheduled scans

You can schedule scans to run at certain times. Users can also schedule scans for their computers from client computers, but they cannot change or disable the scans that you schedule for their computers. The client software runs one scheduled scan at a time. If more than one scan is scheduled at the same time, they run sequentially.

Scheduled scans have settings that are similarly to Auto-Protect scan settings, but each type of scan is configured separately. Centralized exceptions that you configure apply to all types of antivirus and antispyware scans.

If a computer is turned off during a scheduled scan, the scan does not run unless the computer is configured to run missed scan events.

Scheduled scans inspect files for viruses and security risks, such as spyware and adware.

See "Configuring a scheduled scan for Windows clients" on page 448.

See "Setting advanced options for administrator-defined scans" on page 455.

Table 25-3 describes the types of scheduled scans.

Table 25-3 Types of scheduled scans

Type	Description
Active Scan	Scans the system memory and all the common virus and security risk locations on the computer quickly. The scan includes all processes that run in memory, important Windows registry files, and files like config.sys and windows.ini. It also includes some critical operating system folders.
Full Scan	Scans the entire computer for viruses and security risks, including the boot sector and system memory.
Custom Scan	Scans the files and folders that you select for viruses and security risks.

About on-demand scans

You can run an on-demand scan from the console to inspect selected files and folders on selected client computers. On-demand scans provide immediate results from a scan on an area of the network or a local hard drive. You can run these scans from the Client tab in the console. You can also run these scans from the Monitors tab in the console.

See "Running on-demand scans" on page 453.

See "Running commands and actions from logs" on page 274.

The default on-demand scan scans all files and folders. You can change the settings for on-demand scans in an Antivirus and Antispyware Policy. In the policy, you can specify the file extensions and folders that you want to scan. When you run an on-demand scan from the Monitors page, the scan runs on the client based on the settings that are configured in the policy.

See "Configuring an on-demand scan for Windows clients" on page 450.

About TruScan proactive threat scans

TruScan proactive threat scans use heuristics to scan for the behavior that is similar to virus and security risk behavior. Unlike antivirus and antispyware scans, which detect known viruses and security risks, Proactive threat scans detect unknown virus and security risks.

Note: Because proactive threat scanning examines active processes on client computers, the scanning can impact system performance.

The client software runs proactive threat scans by default. You can enable or disable proactive threat scanning in an Antivirus and Antispyware Policy. Users on client computers can enable or disable this type of scan if you do not lock the setting.

Although you include settings for proactive threat scans in an Antivirus and Antispyware Policy, you configure the scan settings differently from antivirus and antispyware scans.

See "About TruScan proactive threat scans" on page 519.

About scanning after updating definitions files

If Auto-Protect is enabled, the client software begins scanning with the updated definitions files immediately.

When definitions files are updated, the client software tries to repair the files that are stored in Quarantine and scans active processes.

For proactive threat scan the detections that are quarantined, the files are scanned to see if they are now considered a virus or security risk. The client scans items quarantined by proactive threat scans similar to how it scans items quarantined by other types of scans. For quarantined detections, the client software completes the remediation and cleans up any side effects. If the proactive threat detection is now part of the Symantec white list, the client software restores and removes the detection from the quarantine; however, the process is not relaunched.

About scanning selected extensions or folders

For each type of antivirus and antispyware scan and Auto-Protect, you can select files to include by extension. For administrator-defined scans, you can also select files to include by folder. For example, you can specify that a scheduled scan only scans certain extensions and that Auto-Protect scans all extensions.

When you select file extensions or folders for scans, you can select multiple extensions or the folders that you want to scan. Any extensions or folders that you do not select are excluded from the scan.

In the File Extensions dialog box, you can quickly add extensions for all common programs or all common documents. You can also add your own extensions. When you add your own extension, you can specify an extension with up to four characters.

In the Edit Folders dialog box, you select Windows folders, rather than absolute folder paths. Client computers in your security network might use different paths to these folders. You can select any of the following folders:

- COMMON_APPDATA

- COMMON_DESKTOPDIRECTORY
- COMMON_DOCUMENTS
- COMMON_PROGRAMS
- COMMON_STARTUP
- PROGRAM_FILES
- PROGRAM_FILES_COMMON
- SYSTEM
- WINDOWS

When you scan selected file extensions or folders, you can improve scan performance. For example, if you copy a large folder that is not in the selected folders list, the copying process is faster because the folder's contents are excluded.

You can exclude files from scans by extension or directory type. You exclude files by configuring a Centralized Exceptions Policy that contains the exclusions. When you specify exclusions in a policy, the exclusions are applied any time any antivirus and antispyware scans run on clients with that policy.

See "Configuring a Centralized Exceptions Policy" on page 579.

When you scan selected extensions, the client software does not read the file header to determine the file type. When you scan selected extensions, the client scans only the files with the extensions that you specify.

Warning: Because the client software excludes files and folders from scans, it does not protect excluded files and folders from viruses and security risks.

Table 25-4 describes the recommended extensions for scanning.

Table 25-4 Recommended file extensions for scanning

File extension	Description
CHM	HTML compiled help file for Microsoft Windows
386	Driver
ACM	Driver; audio compression manager
ACV	Driver; audio compression or decompression manager
ADT	ADT file; fax
AX	AX file

Table 25-4 Recommended file extensions for scanning *(continued)*

File extension	Description
BAT	Batch
BTM	Batch
BIN	Binary
CLA	Java Class
CMD	Command file
COM	Executable
CPL	Applet Control Panel for Microsoft Windows
CSC	Corel Script
CSH	UNIX Shell script
DLL	Dynamic Link Library
DOC	Microsoft Word
DOT	Microsoft Word
DRV	Driver
EXE	Executable
HLP	Help file
HTA	HTML application
HTM	HTML
HTML	HTML
HTT	HTML
INF	Installation script
INI	Initialization file
JPEG	Graphics file
JPG	Graphics file
JS	JavaScript
JSE	JavaScript Encoded

Table 25-4 Recommended file extensions for scanning *(continued)*

File extension	Description
JTD	Ichitaro
MDB	Microsoft Access
MP?	Microsoft Project
MSO	Microsoft Office 2000
OBD	Microsoft Office binder
OBT	Microsoft Office binder
OCX	Microsoft object that links and embeds custom control
OV?	Overlay
PDF	Adobe Portable Document Format
PIF	Program information file
PL	PERL program source code (UNIX)
PM	Presentation Manager Bitmaps Graphics
POT	Microsoft PowerPoint
PPT	Microsoft PowerPoint
PPS	Microsoft PowerPoint
RTF	Rich Text Format document
SCR	Fax, screensaver, snapshot, or script for Farview or Microsoft Windows
SH	Shell Script (UNIX)
SHB	Corel Show Background file
SHS	Shell scrap file
SMM	Lotus AmiPro
SYS	Device driver
VBE	VESA BIOS (Core Functions)
VBS	VBScript

Table 25-4 Recommended file extensions for scanning *(continued)*

File extension	Description
VSD	Microsoft Office Visio
VSS	Microsoft Office Visio
VST	Microsoft Office Visio
VXD	Virtual device driver
WSF	Windows Script File
WSH	Windows Script Host Settings File
XL?	Microsoft Excel
XL??	Microsoft Excel
ACCD?	Microsoft Office Access
DOC?	Microsoft Office Word
DOT?	Microsoft Office Word
PP?	Microsoft Office PowerPoint
PP??	Microsoft Office PowerPoint

About excluding named files and folders

There might be certain security risks that your company's security policy lets you keep on your computers. You can configure the client to exclude these risks from all antivirus and antispyware scans.

You can exclude named files and folders from Auto-Protect and administrator-defined scans. For example, you can exclude the path C:\Temp\Install or folders that contain an allowable security risk. You can exclude the files that trigger false-positive alerts. For example, if you used another virus scanning program to clean an infected file, the program might not completely remove the virus code. The file may be harmless but the disabled virus code might cause the client software to register a false positive. Check with Symantec Technical Support if you are not sure if a file is infected.

When you create an exclusion, it applies to all types of antivirus and antispyware scans that you run. You create an exclusion as part of a centralized exception.

See "Configuring a Centralized Exceptions Policy" on page 579.

About actions for the viruses and the security risks that scans detect on Windows clients

Many of the same scan options are available for different types of scans. However, the actions that you can assign when a scan finds viruses and security risks are different for different client operating systems.

For Windows computers, you can assign the first and second actions that the software takes when an on-demand, scheduled, or Auto-Protect scan finds viruses and security risks.

You can assign individual first and second actions to take when the client discovers the following types of risks:

- Macro viruses
- Non-macro viruses
- All security risks (adware, spyware, joke programs, dialers, hacking tools, remote access programs, trackware, and others)
- Individual categories of security risks, such as spyware
- Custom actions for a particular instance of a security risk

By default, the Symantec Endpoint Protection client first tries to clean a file that is infected by a virus.

If the client software cannot clean the file, it does the following actions:

- Moves the file to the Quarantine on the infected computer
- Denies any access to the file
- Logs the event

By default, the client moves any files that are infected by security risks to the Quarantine on the infected computer. The client also tries to remove or repair the risk's side effects. By default, the Quarantine contains a record of all actions that the client performed. You can return the client computer to the state that existed before the client tried the removal and repair.

If a security risk cannot be quarantined and repaired, the second action is to log the risk.

For TruScan Proactive Threat Scan detections, the actions depend on whether you use Symantec-managed defaults or set the actions yourself. You configure actions for proactive threat scans in a separate part of the antivirus and antispyware Policy.

See "Specifying the actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers" on page 530.

See "About actions for the viruses and the security risks that scans detect on Mac clients" on page 409.

About actions for the viruses and the security risks that scans detect on Mac clients

For Mac client computers, you can choose whether to have the software try to repair any infected files that a scan detects. You can also choose whether to have the software move any infected files that it cannot repair to the Quarantine.

These options are available for scheduled scans and Auto-Protect scans.

See "About actions for the viruses and the security risks that scans detect on Windows clients" on page 408.

Setting up log handling parameters in an Antivirus and Antispyware Policy

You can include log handling parameters in the Antivirus and Antispyware Policy. By default, clients always send certain types of events to the management server (such as **Scan stopped** or **Scan started**). You can choose to send or not send other types of events (such as **File not scanned**).

The events that clients send to the management server affect information in reports and logs. You should decide what types of events that you want to forward to the management server. You can reduce the size of the logs and the amount of information that is included in reports if you select only certain types of events.

You can also configure how long the client retains log items. The option does not affect any events that the clients send to the management console. You can use the option to reduce the actual log size on the client computers.

You can click **Help** for more information about the options that are used in this procedure.

To set up log handling parameters for an Antivirus and Antispyware Policy

1. On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click **Miscellaneous**.
2. On the **Log Handling** tab, under **Antivirus and Antispyware Log Event Filtering**, select the events that you want to forward to the management server.

3 Under **Log Retention**, select how often the client deletes log lines.

4 Under **Log Event Aggregation**, select how often aggregated events are sent to the server.

5 If you are finished with the configuration for this policy, click **OK**.

About client interaction with antivirus and antispyware options

You can configure the specific parameters in the policy that control the client user experience.

You can display and customize warning messages on infected computers. For example, if users have a spyware program installed on their computers, you can notify them that they have violated your corporate policy. You can include a message in the notification that users must uninstall the application immediately.

For both Windows and Mac clients, you can display a warning when definitions are out of date or missing.

For Windows clients, you can also do any of the following actions:

- Configure scan progress options for scheduled scans.
- Set scanning options for clients.
- Change the password that is required to scan mapped drives.
- Specify how Windows Security Center interacts with the Symantec Endpoint Protection client.
- Specify a URL to appear in antivirus and antispyware error notifications.
- Specify a URL to redirect an Internet browser if a security risk tries to change the URL.

Note: You can also lock policy settings so that users cannot change the settings.

Changing the password that is required to scan mapped network drives

Symantec Endpoint Protection requires users on client computers to provide a password before they can scan a mapped network drive. By default, this password is set to symantec.

Note: If users scan network drives, the scan can impact the client computer performance.

You can click Help for more information about the options that are used in the procedure.

To change the password that is required to scan mapped drives

1. On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click **Miscellaneous**.
2. On the **Miscellaneous** tab, under **Scan Network Drive**, check **Ask for password before scanning a mapped network drive**.
3. Click **Change Password**.
4. In the **Configure Password** dialog box, type a new password, and then confirm by typing the password again.
5. Click **OK**.
6. If you are finished with the configuration for this policy, click **OK**.

Configuring Windows Security Center to work with the Symantec Endpoint Protection client

Windows Security Center provides alerts on your client computers if any security software is out of date or if security settings should be strengthened. It is included with Windows XP Service Pack 2, Windows Vista, and Windows 7. You can use an Antivirus and Antispyware Policy to configure some Windows Security Center settings on your client computers that run Windows XP Service Pack 2.

Note: You cannot use an Antivirus and Antispyware Policy to configure Windows Security Center on your client computers that run Windows Vista or Windows 7.

Table 25-5 Options to configure how Windows Security Center works with the client

Option	Description	When to use
Disable Windows Security Center	Lets you permanently or temporarily disable Windows Security Center on your client computers Available options: ■ Never. Windows Security Center is always enabled on the client computer. ■ Once. Windows Security Center is disabled only once. If a user enables it, it is not disabled again. ■ Always. Windows Security Center is permanently disabled on the client computer. If a user enables it, it is immediately disabled. ■ Restore. Windows Security Center is enabled if the Antivirus and Antispyware Policy previously disabled it.	Disable Windows Security Center permanently if you do not want your client users to receive the security alerts that it provides. Client users can still receive Symantec Endpoint Protection alerts. Enable Windows Security Center permanently if you want your client users to receive the security alerts that it provides. You can set Windows Security Center to display Symantec Endpoint Protection alerts.
Display antivirus alerts within Windows Security Center	Lets you set antivirus alerts from the Symantec Endpoint Protection client to appear in the Windows notification area.	Enable this setting if you want your client users to receive Symantec Endpoint Protection alerts together with other security alerts in the Windows notification area of their computers.
Display a Windows Security Center message when definitions are outdated	Lets you set the number of days after which Windows Security Center considers definitions to be outdated. By default, Windows Security Center sends this message after 30 days.	Set this option if you want Windows Security Center to notify your client users about outdated definitions more frequently than the default time (30 days). **Note:** On client computers, the Symantec Endpoint Protection client checks every 15 minutes to compare the out-of-date time, the date of the definitions, and the current date. Typically, no out-of-date status is reported to Windows Security Center because definitions are usually updated automatically. If you update definitions manually you might have to wait up to 15 minutes to view an accurate status in Windows Security Center.

To configure Windows Security Center to work with Symantec Endpoint Protection

1. On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click **Miscellaneous**.
2. Under **Windows Security Center**, set the options that your company's security policies require.

Note: Symantec product status is always available in the management console, regardless of whether Windows Security Center is enabled or disabled.

Displaying a warning when definitions are out of date or missing

You can display and customize warning messages to appear on client computers when their virus and security risk definitions are outdated or missing. You might want to alert users if you do not have automatic updates scheduled.

To display a warning about definitions

1. On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click **Miscellaneous**.
2. On the **Notifications** tab, under **Notifications**, select one or both of the following options:
   - **Display a warning when definitions are outdated**
   - **Display a warning when Symantec Endpoint Protection is running without virus definitions**
3. For outdated virus and security risk definitions, set the number of days that definitions can be outdated before the warning appears.
4. For missing virus and security risk definitions, set the number of remediation tries that Symantec Endpoint Protection must make before the warning appears.
5. Click **Warning** for each option that you checked, and then customize the default message.
6. In the warning dialog box, click **OK**.
7. If you are finished with the configuration for this policy, click **OK**.

Specifying a URL to appear in antivirus and antispyware error notifications

In rare cases, users might see errors appear on client computers. For example, the client computer might encounter buffer overruns or decompression problems during scans.

You can specify a URL that points to the Symantec support Web site or to a custom URL. For example, you might have an internal Web site that you want to specify instead.

Note: The URL also appears in the system event log for the client computer on which the error occurs.

To specify a URL to appear in antivirus and antispyware error notifications

1. On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click **Miscellaneous**.
2. On the **Notifications** tab, check **Display error messages with a URL to a solution**.
3. Select one of the following options:
   - **Display the URL to a Symantec Technical Support Knowledge Base article**
   - **Display a custom URL**
4. Click **Customize Error Message** if you want to customize the message.
5. Enter the custom text that you want to include, and then click **OK**.
6. If you are finished with the configuration for this policy, click **OK**.

Specifying a URL for a browser home page

You can specify a URL to use as the home page when the Symantec Endpoint Protection client repairs a security risk that hijacked a browser home page.

To specify a URL for a browser home page

1. On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click **Miscellaneous**.
2. On the **Miscellaneous** tab, under **Internet Browser Protection**, type the URL.
3. If you are finished with the configuration for this policy, click **OK**.

Configuring the options that apply to antivirus and antispyware scans

Some scanning options are common to all antivirus and antispyware scans. Antivirus and antispyware scans include both Auto-Protect and administrator-defined scans.

The policy includes the following options:

- Configure scans of selected file extensions or folders.
- Configure centralized exceptions for security risks.
- Configure actions for known virus and security risk detections.
- Manage notification messages on infected computers.
- Customize and display notifications on infected computers.
- Add warnings to infected email messages.
- Notify senders of infected email messages.
- Notify users of infected email messages.

Information about actions and notifications for proactive threat scans is included in a separate section.

See "Configuring notifications for TruScan proactive threat scans" on page 532.

Configuring scans of selected file extensions

The Symantec Endpoint Protection client may complete scans faster by scanning only files with selected extensions. Scans that scan only selected extensions offer less protection to computers; however, when you scan only selected extensions you can select the file types that viruses typically attack. When you scan selected extensions, you can make scans more efficient and use less of the computer's resources.

You can configure the extensions to scan to balance the following requirements:

- The amount of protection that your network requires
- The amount of time and resources that are required to provide the protection

For example, you might want to scan only the files with the extensions that are likely to contain a virus or other risk. When you scan only certain extensions, you automatically exclude all files with other extensions from the scan. When you exclude files from scans, you decrease the amount of computer resources that are required to run the scan.

Warning: When you select extensions that you want to scan, any other extensions are not protected from viruses and security risks.

You can click **Help** for more information about the options that are used in the procedure.

To include only files with particular extensions for Auto-Protect or administrator-defined scans

1. On the **Scan Details** tab, under **File types**, click **Scan only selected extensions**.
2. Click **Select Extensions**.
3. In the **File Extensions** dialog box, you can do any of the following:
   - To add your own extensions, type the extension, and then click **Add**.
   - To remove any extensions, select the extensions, and then click **Remove**.
   - To return the list to its default setting, click **Use Defaults**.
   - To add all program extensions, click **Add Common Programs**.
   - To add all document extensions, click **Add Common Documents**.
4. If you are finished with the configuration for this policy, click **OK**.

Configuring the scans of selected folders

You can configure selected folders for certain administrator-defined scans to scan. These administrator-defined scans include custom scheduled scans and on-demand scans. You cannot configure selected folders for Auto-Protect.

See "About scanning selected extensions or folders" on page 403.

You can click **Help** for more information about the options that are used in this procedure.

To configure the scans of selected folders

1. On the **Antivirus and Antispyware Policy** page, click **Administrator-defined Scan**.
2. On the **Scans** tab, do one of the following:
   - Click **Add**.
   - Under **Scheduled scans**, select an existing scan, and then click **Edit**.
   - Under **Administrator On-demand Scan**, click **Edit**.
3. On the **Scan Details** tab, in the **Scan type** drop-down list, click **Custom Scan**.

   On-demand scans are preset to Custom Scan.

4 Under **Scanning**, click **Edit Folders**.

5 In the **Edit Folders** dialog box, click **Scan selected folders**, and then in the folder list, check all the folders that you want this scan to scan.

The **Selected folders** field shows all of your choices.

6 Click **OK** until you return to the **Administrator-defined Scan** page.

7 If you are finished with the configuration for this policy, click **OK**.

About exceptions for security risks

If you want any security risks to remain on your network, you can ignore the security risks when they are detected on client computers.

If a user has configured custom actions for a security risk that you have specified to ignore, the user's custom actions are not used.

Note: When you add a security risk to the exceptions list, the Symantec Endpoint Protection client no longer logs any events that involve that security risk. You can configure the client to log the risk even if you include the risk in the exceptions list. Regardless of whether the risk is logged or not, users are not notified in any way when the risk is present on their computers.

You can use a **Centralized Exceptions** Policy to configure exceptions.

See "Configuring a Centralized Exceptions Policy" on page 579.

Configuring actions for known virus and security risk detections on Windows clients

You use actions to specify how clients respond when an antivirus and antispyware scan detects a known virus or security risk. These actions apply to Auto-Protect and administrator-defined scans. You configure actions for proactive threat scans separately.

See "About TruScan proactive threat scans" on page 519.

Actions let you set how the client software responds when it detects a known virus or a security risk. For Windows client computers, you can assign a first action and, in case the first action is not possible, a second action. The Symantec Endpoint Protection client uses these actions when it discovers a virus or a security risk such as adware or spyware. Types of viruses and security risks are listed in the hierarchy.

You configure actions differently for Mac client computers.

See "Configuring actions for known virus and security risk detections on Mac clients" on page 418.

You can click **Help** for more information about the options that are used in the procedures.

Note: For security risks, use the delete action with caution. In some cases, deleting security risks causes applications to lose functionality.

Warning: If you configure the client software to delete the files that security risks affect, it cannot restore the files.

To back up the files that security risks affect, configure the client software to quarantine them.

To configure actions for known virus and security risk detections on Windows clients

1. On the **Actions** tab, under **Detection**, select a type of virus or security risk.

   By default, each security risk subcategory is automatically configured to use the actions that are set for the entire **Security Risks** category.
2. To configure a specific instance of a security risk category to use different actions, check **Override actions configured for Security risks**, and then set the actions for that category only.
3. Under **Actions for**, select the first and second actions that the client software takes when it detects that category of virus or security risk.

   You can lock actions so that users cannot change the action on the client computers that use this policy.

   For security risks, use the Delete action with caution. In some cases, deleting security risks causes applications to lose functionality.
4. Repeat step 3 for each category for which you want to set actions (viruses and security risks).
5. When you finish configuring this policy, click **OK**.

Configuring actions for known virus and security risk detections on Mac clients

You use actions to specify how clients respond when an antivirus and antispyware scan detects a known virus or security risk. These actions apply to Auto-Protect and administrator-defined scans.

For Mac client computers, you choose whether to repair files, and whether to quarantine files that cannot be repaired.

You configure actions differently for Windows computers.

See "Configuring actions for known virus and security risk detections on Windows clients" on page 417.

To configure actions for known virus and security risk detections on Mac clients

1. On the **Common Settings** tab, under **Actions**, check either of the following options:
   - **Automatically repair infected files**
   - **Quarantine files that cannot be repaired**

   You can lock actions so that users cannot change the action on the client computers that use this policy.
2. When you finish configuring this policy, click **OK**.

About notification messages on infected computers

You can enable a custom notification message to appear on infected computers when an administrator-defined scan or Auto-Protect finds a virus or security risk. These notifications can alert users to review their recent activity on the client computer. For example, a user might download an application or view a Web page that results in a spyware infection.

Also, you can display the **Scan Results** dialog box on the infected computer when a File System Auto-Protect scan finds a virus or security risk.

Note: The language of the operating system on which you run the client might not be able to interpret some characters in virus names. If the operating system cannot interpret the characters, the characters appear as question marks in notifications. For example, some Unicode virus names might contain double-byte characters. On the computers that run the client on an English operating system, these characters appear as question marks.

For Auto-Protect scans of email, you can also configure the following options:

- **Insert a warning into the email message**
- **Send email to the sender**
- **Send email to others**.

See "Configuring notification options for Auto-Protect" on page 440.

Notifications for proactive threat scan results are configured separately.

See “Configuring notifications for TruScan proactive threat scans” on page 532.

Customizing and displaying notifications on infected computers

You can construct a custom message to appear on infected computers when a virus or a security risk is found. You can type directly in the message field to add or modify the text.

When you run a remote scan, you can notify the user of a problem by displaying a message on the infected computer's screen. You can customize the warning message by including information such as the name of the risk, the name of an infected file, and the status of the risk. A warning message might look like the following example:

```
Scan type: Scheduled Scan
Event: Risk Found
SecurityRiskName: Stoned-C
File: C:\Autoexec.bat
Location: C:
Computer: ACCTG-2
User: JSmith
Action taken: Cleaned
```

Table 25-6 describes the variable fields that are available for notifications.

Table 25-6 Notification message fields

Label	Field	Description
Scan type	**LoggedBy**	The type of scan, on-demand, scheduled, and so on, that detected the virus or security risk.
Event	**Event**	The type of event, such as “Risk Found.”
Security risk detected	**SecurityRiskName**	The name of the virus or security risk that was found.
File	**PathAndFilename**	The complete path and name of the file that the virus or the security risk has infected.

Table 25-6 Notification message fields *(continued)*

Label	Field	Description
Location	**Location**	The drive on the computer on which the virus or security risk was located.
Computer	**Computer**	The name of the computer on which the virus or security risk was found.
User	**User**	The name of the user who was logged on when the virus or security risk occurred.
Action taken	**ActionTaken**	The action that was taken in response to detecting the virus or security risk. This action can be either the first action or second action that was configured.
Date found	**DateFound**	The date on which the virus or security risk was found.

To display notification messages on infected computers

1. On the **Antivirus and Antispyware Policy** page, click one of the following options:
   - **Administrator-defined Scans**
   - **File System Auto-Protect**
   - **Internet Email Auto-Protect**
   - **Microsoft Outlook Auto-Protect**
   - **Lotus Notes Auto-Protect**
2. If you selected **Administrator-defined Scans**, on the **Scans** tab, click **Add** or **Edit**.
3. On the **Notifications** tab, check **Display a notification message on the infected computer** and modify the body of the notification message.
4. Click **OK**.

Submitting information about scans to Symantec

You can specify that information about proactive threat scan detections and information about Auto-Protect or scan detections are automatically sent to Symantec Security Response.

Information that clients submit helps Symantec determine if a detected threat is real. If Symantec determines the threat is real, Symantec can generate a signature to address the threat. The signature is included in an updated version of definitions. For TruScan proactive threat detections, Symantec can update its lists of allowed or disallowed processes.

When a client sends information about a process, the information includes the following items:

- The path to the executable
- The executable
- The internal state information
- The information about the file and the Windows registry load points that refer to the threat
- The content version that the proactive threat scan used

Any personal information that can identify the client computer is not submitted.

Information about detection rates potentially helps Symantec refine virus definitions updates. Detection rates show the viruses and security risks that are detected most by customers. Symantec Security Response can remove the signatures that are not detected, and provide a segmented virus definition list for the customers who request it. Segmented lists increase antivirus and antispyware scan performance.

When a proactive threat scan makes a detection, the client software checks to see if information about the process has already been sent. If the information has been sent, the client does not send the information again.

Note: When proactive threat scans detect items on the commercial applications list, the information about these detections is not forwarded to Symantec Security Response.

When you enable submission for processes, items that are quarantined by proactive threat scans are updated. When the items are updated, the Quarantine window shows that the samples have been submitted to Symantec Security Response. The client software does not notify users and the management console does not give

an indication when detections with other types of actions are submitted. Other types of actions include Log or Terminate.

You can submit Quarantine samples to Symantec.

See "Submitting quarantined items to Symantec" on page 427.

About submissions throttling

Clients may or may not submit samples to Symantec depending on the following information:

- The date of the Submission Data Control file
- The percentage of the computers that are allowed to send submissions

Symantec publishes its Submission Control Data (SCD) file and includes it as part of a LiveUpdate package. Each Symantec product has its own SCD file.

The file controls the following settings:

- How many submissions a client can submit in one day
- How long to wait before the client software retries submissions
- How many times to retry failed submissions
- Which IP address of the Symantec Security Response server receives the submission

If the SCD file becomes out-of-date, then clients stop sending submissions. Symantec considers the SCD file out-of-date when a client computer has not retrieved LiveUpdate content in 7 days.

If clients stop the transmission of the submissions, the client software does not collect the submission information and send it later. When clients start to transmit submissions again, they only send the information about the events that occur after the transmission restart.

Administrators can also configure the percentage of computers that are allowed to submit. Each client computer determines whether or not it should submit information. The client computer randomly selects a number from 1 to 100. If the number is less than or equal to the percentage that is set in that computer's policy, then the computer submits information. If the number is greater than the configured percentage, the computer does not submit information.

Configuring submissions options

You can enable or disable submissions for Windows clients in an Antivirus and Antispyware Policy. Submissions are enabled by default.

You can click **Help** for more information about the options that are used in this procedure.

To specify whether or not information is sent about processes detected by TruScan proactive threat scans

1. On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click **Submissions**.
2. Under **TruScan Proactive Threat Scans**, check or uncheck **Allow client computers to submit processes detected by scans**.
3. When you check this parameter, you can change the percentage of client computers that are allowed to submit information about processes.
4. If you enabled submissions, use the up arrow or down arrow to select the percentage or type the desired value in the text box.
5. If you are finished with the configuration for this policy, click **OK**.

To specify whether or not information is sent about Auto-Protect and manual scan detection rates

1. On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click **Submissions**.
2. Under **Detection Rates**, check or uncheck **Allow client computers to submit threat detection rates**.

   When you check this parameter, you can change the percentage of client computers that are allowed to submit detection rates.
3. If you are finished with the configuration for this policy, click **OK**.

Managing quarantined files

Managing quarantined files includes the following:

- Specifying a local quarantine directory
- Submitting quarantined items to Symantec
- Configuring actions to take when new definitions arrive

About Quarantine settings

You use the Antivirus and Antispyware Policy to configure client Quarantine settings.

You manage Quarantine settings as an important part of your virus outbreak strategy.

Specifying a local Quarantine directory

If you do not want to use the default quarantine directory to store quarantined files on client computers, you can specify a different local directory. You can use path expansion by using the percent sign when you type the path. For example, you can type %COMMON_APPDATA%. Relative paths are not allowed.

The software supports the following expansion parameters:

%COMMON_APPDATA%	This path is typically C:\Documents and Settings\All Users\Application Data
%PROGRAM_FILES%	This path is typically C:\Program Files
%PROGRAM_FILES_COMMON%	This path is typically C:\Program Files\Common
%COMMON_PROGRAMS%	This path is typically C:\Documents and Settings\All Users\Start Menu\Programs
%COMMON_STARTUP%	This path is typically C:\Documents and Settings\All Users\Start Menu\Programs\Startup
%COMMON_DESKTOPDIRECTORY%	This path is typically C:\Documents and Settings\All Users\Desktop
%COMMON_DOCUMENT%	This path is typically C:\Documents and Settings\All Users\Documents
%SYSTEM%	This path is typically C:\Windows\System32
%WINDOWS%	This path is typically C:\Windows

To specify a local quarantine directory

1. On the Antivirus and Antispyware Policy page, click **Quarantine**.
2. On the Miscellaneous tab, under Local Quarantine Options, click **Specify Quarantine Directory**.
3. In the text box, type the name of a local directory on the client computers. You can use path expansion by using the percent sign when typing in the path. For example, you can type %COMMON_APPDATA%, but relative paths are not allowed.
4. If you are finished with the configuration for this policy, click **OK**.

Configuring automatic clean-up options

When the client software scans a suspicious file, it places the file in the local Quarantine folder on the infected computer. The Quarantine clean-up feature automatically deletes the files in the Quarantine when they exceed a specified age. The Quarantine clean-up feature automatically deletes the files in the Quarantine when the directory where they are stored reaches a certain size.

You can configure these options using the Antivirus and Antispyware Policy. You can individually configure the number of days to keep repaired, backup, and quarantined files. You can also set the maximum directory size that is allowed before files are automatically removed from the client computer.

You can use one of the settings, or you can use both together. If you set both types of limits, then all files older than the time you have set are purged first. If the size of the directory still exceeds the size limit that you set, then the oldest files are deleted one by one. The files are deleted until the directory size falls below the limit. By default, these options are not enabled.

To configure automatic clean-up options

1. On the **Antivirus and Antispyware Policy** page, click **Quarantine**.
2. On the **Cleanup** tab, under **Repaired files**, check or uncheck **Enable automatic deleting of repaired files**.
3. In the **Delete after** box, type a value or click an arrow to select the time interval in days.
4. Check **Delete oldest files to limit folder size at**, and then type in the maximum directory size, in megabytes. The default setting is 50 MB.
5. Under **Backup Files**, check or uncheck **Enable automatic deleting of backup files**.
6. In the **Delete after** box, type or click an arrow to select the time interval in days.
7. Check **Delete oldest files to limit folder size at**, and then type the maximum directory size, in megabytes. The default is 50 MB.
8. Under **Quarantined Files**, check or uncheck **Enable automatic deleting of quarantined files that could not be repaired**.
9. In the **Delete after** box, type a value or click an arrow to select the time interval in days.
10. Check **Delete oldest files to limit folder size at**, and then type in the maximum directory size, in megabytes. The default is 50 MB.
11. If you are finished with the configuration for this policy, click **OK**.

Submitting quarantined items to a central Quarantine Server

You can enable items in Quarantine to be forwarded from the local Quarantine to a Central Quarantine Server. You should configure the client to forward items if you use a Central Quarantine Server in your security network. The Central Quarantine Server can forward the information to Symantec Security Response. Information that clients submit helps Symantec determine if a detected threat is real.

Note: Only the quarantined items that are detected by antivirus and antispyware scans may be sent to a Central Quarantine Server. Quarantined items that are detected by proactive threat scans cannot be sent.

To enable submission of quarantined items to a Quarantine Server

1. On the Antivirus and Antispyware Policy page, click **Submissions**.
2. Under Quarantined Items, check **Allow client computers to automatically submit quarantined items to a Quarantine Server**.
3. Type the name of the Quarantine Server.
4. Type the port number to use, and then select the number of seconds to retry connecting.
5. If you are finished configuring settings for this policy, click **OK**.

Submitting quarantined items to Symantec

You can enable the client software to allow users to submit infected or suspicious files and related side effects to Symantec Security Response for further analysis. When users submit information, Symantec can refine its detection and repair.

Files that are submitted to Symantec Security Response become the property of Symantec Corporation. In some cases, files may be shared with the antivirus community. If Symantec shares files, Symantec uses industry-standard encryption and may make data anonymous to help protect the integrity of the content and your privacy.

See "Submitting information about scans to Symantec" on page 422.

In some cases, Symantec might reject a file. For example, Symantec might reject a file because the file does not seem to be infected. You can enable the resubmission of files if you want users to be able to resubmit selected files. Users can resubmit files once per day.

To enable submission of quarantined items to Symantec

1. On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click **Submissions**.
2. Under **Quarantined Items**, check **Allow client computers to manually submit quarantined items to Symantec Security Response**.
3. If you are finished with the configuration for this policy, click **OK**.

Configuring actions to take when new definitions arrive

You can configure the actions that you want to take when new definitions arrive on client computers. By default, the client rescans items in the Quarantine and automatically repairs and restores items silently. Typically, you should always use this setting.

To configure actions for new definitions

1. On the Antivirus and Antispyware Policy page, click **Quarantine**.
2. On the General tab, under When new virus definitions arrive, click one of the following options:
   - **Automatically repair and restore files in Quarantine silently**
   - **Repair files in Quarantine silently without restoring**
   - **Prompt user**
   - **Do nothing**
3. If you are finished with the configuration for this policy, click **OK**.

Chapter 26

Configuring Auto-Protect

This chapter includes the following topics:

About configuring Auto-Protect

You configure Auto-Protect settings as part of an Antivirus and Antispyware Policy. You can also manually enable Auto-Protect for a client group or particular computers and users.

You can lock or unlock many Auto-Protect options in an Antivirus and Antispyware Policy. When you lock an option, users on client computers cannot change the option. By default, options are unlocked.

Some options for Auto-Protect are similar to options for other antivirus and antispyware scans.

See "Configuring the options that apply to antivirus and antispyware scans" on page 415.

About types of Auto-Protect

Auto-Protect protects both the file system and the email attachments that clients receive.

You can configure the following types of Auto-Protect:

- File System Auto-Protect
- Internet Email Auto-Protect
- Microsoft Outlook Auto-Protect
- Lotus Notes Auto-Protect

By default, all types of Auto-Protect are enabled. If your client computers run other email security products, such as Symantec Mail Security, you might not need to enable Auto-Protect for email.

See "About Auto-Protect scans" on page 396.

Enabling File System Auto-Protect

Auto-Protect settings are included in the Antivirus and Antispyware Policy that you apply to the client computers. By default, File System Auto-Protect is enabled. You can lock the setting so that users on client computers cannot disable File System Auto-Protect. You might need to enable Auto-Protect from the console if you allow users to change the setting or if you disable File System Auto-Protect.

You can enable File System Auto-Protect by using the Clients tab in the console. You can also manually enable File System Auto-Protect from the computer status logs.

See "Running commands and actions from logs" on page 274.

If you want to disable Auto-Protect, you must disable the setting in the Antivirus and Antispyware Policy that is applied to the group.

To enable File System Auto-Protect

1. In the console, click **Clients**, and then under View Clients, select the group that includes computers for which you want to enable Auto-Protect.
2. In the right pane, select the Clients tab.
3. Do one of the following actions:
   - In the left pane, under View Clients, right-click the group for which you want to enable Auto-Protect.
   - In the right pane, on the Clients tab, select the computers and users for which you want to enable Auto-Protect, and then right-click the selection.

4 Click one of the following commands:

- **Run Command on Group > Enable Auto-Protect**
- **Run Command on Clients > Enable Auto-Protect**

5 In the message that appears, click **OK**.

If you want to enable or disable Auto-Protect for email, you must include the setting in the Antivirus and Antispyware Policy.

Configuring File System Auto-Protect for Windows clients

When you configure File System Auto-Protect as part of an Antivirus and Antispyware Policy, you configure the settings that define how Auto-Protect and its associated features behave. You specify whether you want to scan floppy disk drives, network drives, or both.

Note: You configure File System Auto-Protect for Mac clients separately.

See "Configuring File System Auto-Protect for Mac clients" on page 435.

Note: When you configure Auto-Protect options, you can click the lock icon next to the Auto-Protect settings. Users with the client computers that use this policy cannot change the locked settings.

You can click Help for more information about the options that are used in the procedures.

To configure File System Auto-Protect

1 On the Antivirus and Antispyware Policy page, under **Windows Settings**, click **File System Auto-Protect**.

2 On the Scan Details tab, check or uncheck **Enable File System Auto-Protect**.

3 Under Scanning, under File types, click one of the following options:

- **Scan all files**
- **Scan only selected extensions**

See "Configuring scans of selected file extensions" on page 415.

4 Under Additional options, check or uncheck **Scan for security risks** and **Block security risk from being installed**.

See "About Auto-Protect security risk scanning and blocking" on page 432.

5 Under Network Settings, check or uncheck **Network** to enable or disable Auto-Protect scans of network files.

6 If you checked Network, click **Network Settings**.

7 In the Network Settings dialog box, do any of the following actions:

- Enable or disable Auto-Protect to trust files on the remote computers that run Auto-Protect.
- Configure network cache options for Auto-Protect scans.

8 Click **OK**.

9 Under Floppy Settings, check or uncheck **Check floppies for boot viruses when accessed**.

10 If you checked **Check floppies for boot viruses when accessed**, set the action you want to be taken when a boot virus is found. You can either clean it from the boot record or log it and leave it alone.

11 On the Actions tab, set any of the options.

See "Configuring actions for known virus and security risk detections on Windows clients" on page 417.

You can also set remediation options for File System Auto-Protect.

12 On the Notifications tab, set any of the notification options.

See "Configuring notification options for Auto-Protect" on page 440.

13 On the Advanced tab, set any of the following options:

- Startup and shutdown
- Reload options

14 Under Additional Options, click **File Cache** or **Risk Tracer**.

15 Configure the file cache or Risk Tracer settings, and then click **OK**.

16 If you are finished with the configuration for this policy, click **OK**.

About Auto-Protect security risk scanning and blocking

By default, Auto-Protect does the following actions:

- Scans for security risks such as adware and spyware
- Quarantines the infected files

- Removes or repairs the side effects of the security risks

In cases where blocking the installation of a security risk does not affect the stability of a computer, Auto-Protect also blocks the installation by default. If Symantec determines that blocking a security risk could compromise a computer's stability, then Auto-Protect allows the risk to install. Auto-Protect also immediately takes the action that is configured for the risk.

From time to time, however, you might temporarily need to disable scanning for security risks in Auto-Protect, and then enable it. You might also need to disable blocking security risks to control the time at which Auto-Protect reacts to certain security risks.

Note: You cannot disable security risk scanning for other types of scans. However, you can configure Symantec Endpoint Protection to leave the security risk alone and log the detection. You can also exclude specific risks globally from all types of scans by adding them to the centralized exceptions list.

See "About Centralized Exceptions Policies" on page 575.

Configuring advanced scanning and monitoring options

You can configure advanced scanning and monitoring options for Auto-Protect scans of files and processes. The options include when to scan files, and heuristic scanning settings.

Heuristic scanning as part of Auto-Protect is different from proactive threat scanning. Heuristic scanning as part of Auto-Protect scans files for malicious behavior, while proactive threat scanning inspects running processes for malicious behavior.

See "About TruScan proactive threat scans" on page 519.

You can click Help for more information about the options that are used in the procedures.

To configure advanced scanning and monitoring options

1. On the Antivirus and Antispyware Policy page, click **File System Auto-Protect**.
2. On the Scan Details tab, under Scanning, click **Advanced Scanning and Monitoring**.
3. Under Scan Files When, specify what activities trigger scans.
4. Under Bloodhound(TM) Detection Settings, check or uncheck **Enable Bloodhound(TM) virus detection**.

   You can also change the level of protection.

5 Click **OK**.

6 If you are finished with the configuration for this policy, click **OK**.

About Risk Tracer

Risk Tracer identifies the source of network share-based virus infections on your client computers.

When Auto-Protect detects an infection, it sends information to Rtvscan, the main Symantec Endpoint Protection service. Rtvscan determines if the infection originated locally or remotely.

If the infection came from a remote computer, Rtvscan can do the following actions:

- Look up and record the computer's NetBIOS computer name and its IP address.
- Look up and record who was logged on to the computer at delivery time.
- Display the information in the Risk properties dialog box.

Rtvscan polls every second by default for network sessions, and then caches this information as a remote computer secondary source list. This information maximizes the frequency with which Risk Tracer can successfully identify the infected remote computer. For example, a risk may close the network share before Rtvscan can record the network session. Risk Tracer then uses the secondary source list to try to identify the remote computer. You can configure this information in the Auto-Protect Advanced Options dialog box.

Risk Tracer information appears in the Risk Properties dialog box, and is available only for the risk entries that the infected files cause. When Risk Tracer determines that the local host activity caused an infection, it lists the source as the local host.

Risk Tracer lists a source as unknown when the following conditions are true:

- It cannot identify the remote computer.
- The authenticated user for a file share refers to multiple computers. This condition can occur when a user ID is associated with multiple network sessions. For example, multiple computers might be logged on to a file sharing server with the same server user ID.

You can record the full list of multiple remote computers that currently infect the local computer. Set the HKEY_LOCAL_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\ProductControl\Debug string value to “THREATTRACER X” on the local client computer. The THREATTRACER value turns on the debug output and the X ensures that only the debug output for Risk Tracer appears. You can also add an L to ensure that the logging goes to the

<SAV_Program_Folder>\vpdebug.log log file. To ensure that the debug window does not appear, add XW.

If you want to experiment with this feature, use the test virus file Eicar.com available from the following URL:

www.eicar.org

Risk Tracer also includes an option to block the IP addresses of source computers. For this option to take effect, you must set the corresponding option in the Firewall Policy to enable this type of automatic blocking.

See "Configuring File System Auto-Protect for Windows clients" on page 431.

About the file cache

File System Auto-Protect uses a file cache so that it remembers the clean files from the last scan. The file cache persists across startups. If the client computer shuts down and restarts, File System Auto-Protect remembers the clean files and does not scan them.

File System Auto-Protect rescans the files in the following situations:

- The client computer downloads new definitions.
- Auto-Protect detects that the files might have changed when Auto-Protect was not running.

You can disable the file cache if you always want Auto-Protect to scan every file. If you disable the file cache, you might impact the performance of your client computers.

You can also set the following parameters:

- The file cache size
  The default cache size is 10,000 files per volume. You can change the cache size if you want File System Auto-Protect to rescan more or fewer files.
- Whether or not Auto-Protect rescans the cache when new definitions load
  You might want to disable this parameter to improve File System Auto-Protect performance.
  See "Configuring File System Auto-Protect for Windows clients" on page 431.

Configuring File System Auto-Protect for Mac clients

You configure File System Auto-Protect as part of an Antivirus and Antispyware policy. You configure the settings that define how Auto-Protect and its associated features behave. For Mac clients, you specify the following: the files and folders to scan, and whether to scan mounted disks or devices.

- The actions that Auto-Protect takes when it finds a risk
- The files and folders to scan, or to exclude from scans
- How or whether to scan mounted disks or devices

Note: You configure File System Auto-Protect for Windows clients separately.

See "Configuring File System Auto-Protect for Windows clients" on page 431.

You can click Help for more information about the options that are used in the procedures.

To configure File System Auto-Protect for Mac clients

1. On the Antivirus and Antispyware policy page, under **Mac Settings**, click **File System Auto-Protect**.
2. At the top of the **Scan Details** tab, click the lock icon to lock or unlock all File System Auto-Protect settings.
3. Check or uncheck any of the following options:
   - **Enable File System Auto-Protect**
   - **Automatically repair infected files**
   - **Quarantine files that cannot be repaired**
   - **Scan compressed files**
4. Under **General Scan Details**, specify the files that Auto-Protect scans.

   Note: To exclude files from the scan, you must select **Scan everywhere except in specified folders**, and then add a Centralized Exceptions policy to specify the files to exclude.

   See "Configuring a centralized exception for files or folders on Mac clients" on page 583.

   ---

5. Under **Scan Mounted Disk Details**, check or uncheck any of the available options. For more information, see the Help.
6. On the **Notifications** tab, set any of the notification options, and then click **OK**.

   See "Configuring notification options for Auto-Protect" on page 440.

Configuring Internet Email Auto-Protect

Internet Email Auto-Protect protects both incoming email messages and outgoing email messages that use the POP3 or SMTP communications protocol over the Secure Sockets Layer (SSL). When Internet Email Auto-Protect is enabled, the client software scans both the body text of the email and any attachments that are included.

You can enable Auto-Protect to support the handling of encrypted email over POP3 and SMTP connections. Auto-Protect detects the secure connections and does not scan the encrypted messages. Even if Internet Email Auto-Protect does not scan encrypted messages, it continues to protect computers from viruses and security risks in attachments.

File System Auto-Protect scans email attachments when you save the attachments to the hard drive.

Note: Internet Email Auto-Protect is not supported for 64-bit computers. Internet Email Auto-Protect also does not support scanning of POP3 email on server operating systems.

The Symantec Endpoint Protection client also provides outbound email heuristics scanning. The heuristics scanning uses Bloodhound Virus Detection to identify the risks that may be contained in outgoing messages. When the client scans outgoing email messages, the scan helps to prevent the spread of risks. These risks include the worms that can use email clients to replicate and distribute themselves across a network.

Email scanning does not support the following email clients:

- IMAP clients
- AOL clients
- HTTP-based email such as Hotmail and Yahoo! Mail

You can click **Help** for more information about the options that are used in the procedures.

To configure Internet Email Auto-Protect

1. On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click **Internet Email Auto-Protect**.
2. On the **Scan Details** tab, check or uncheck **Enable Internet Email Auto-Protect**.
3. Under **Scanning**, under **File types**, click one of the following options:

- **Scan all files**
- **Scan only selected extensions**

See "Configuring scans of selected file extensions" on page 415.

4 Check or uncheck **Scan files inside compressed files**.

5 Click **OK**

6 On the **Actions** tab, set any of the options.

See "Configuring actions for known virus and security risk detections on Windows clients" on page 417.

7 Click **OK**.

8 On the **Notifications** tab, under **Email Notifications**, check or uncheck any of the following options:

- **Insert a warning into the email message**
- **Send email to the sender**
- **Send email to others**

See "Configuring notification options for Auto-Protect" on page 440.

9 Click **OK**.

10 On the **Advanced** tab, under **Encrypted Connections**, enable or disable encrypted POP3 or SMTP connections.

11 Under **Mass Mailing Worm Heuristics**, check or uncheck **Outbound worm heuristics**.

12 If you are finished with the configuration for this policy, click **OK**.

Configuring Microsoft Outlook Auto-Protect

By default, Auto-Protect scans Microsoft Outlook email attachments. You can customize the scan settings.

You can click **Help** for more information about the options that are used in the procedures.

To configure Microsoft Outlook Auto-Protect

1 On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click **Microsoft Outlook Auto-Protect**.

2 On the **Scan Details** tab, check or uncheck **Enable Microsoft Outlook Auto-Protect**.

3 Under **Scanning**, under **File types**, click one of the following options:

- **Scan all files**
- **Scan only selected extensions**

See "Configuring scans of selected file extensions" on page 415.

4 Check or uncheck **Scan files inside compressed files**.

5 On the **Actions** tab, set any of the options.

See "Configuring actions for known virus and security risk detections on Windows clients" on page 417.

6 On the **Notifications** tab, check or uncheck of the following options:

- **Insert a warning into the email message**
- **Send email to the sender**
- **Send email to others**

See "Configuring notification options for Auto-Protect" on page 440.

7 If you are finished with the configuration for this policy, click **OK**.

Configuring Lotus Notes Auto-Protect

By default, Auto-Protect scans Lotus Notes email attachments. You can customize the scan settings.

You can click **Help** for more information about the options that are used in the procedures.

To configure Lotus Notes Auto-Protect

1 On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click **Lotus Notes Auto-Protect**.

2 On the **Scan Details** tab, check or uncheck **Enable Lotus Notes Auto-Protect**.

3 Under **Scanning**, under **File types**, click one of the following options:

- **Scan all files**
- **Scan only selected extensions**

See "Configuring scans of selected file extensions" on page 415.

4 Check or uncheck **Scan files inside compressed files**.

5 On the **Actions** tab, set any of the options.

See "Configuring actions for known virus and security risk detections on Windows clients" on page 417.

6 On the **Notifications** tab, check or uncheck any of the following options:

- **Insert a warning into the email message**
- **Send email to the sender**
- **Send email to others**

See "Configuring notification options for Auto-Protect" on page 440.

7 If you are finished configuring policy settings, click **OK**.

Configuring notification options for Auto-Protect

By default, the results of File System Auto-Protect scans appear on infected computers. You can configure the Antivirus and Antispyware Policy so that results do not appear on client computers.

You can customize the notification message that appears on client computers when Auto-Protect makes a detection.

See "Customizing and displaying notifications on infected computers" on page 420.

For supported email software, you can also configure Auto-Protect to do the following actions:

- **Insert a warning into the email message**
- **Send email to the sender**
- **Send email to others**.

You can customize the email messages that you send to notify users.

Note: Use caution when you configure the options to notify senders and others about infected email messages. The address of the infected email message might be spoofed. If you send notifications, you might generate spam and cause increased traffic on your network.

The variable fields that you customize for notifications messages and email messages are slightly different. You can customize the information in the message body and the information in the infection field.

Table 26-1 describes the types of information that you can customize for the message body.

Table 26-1 Email message body fields

Field	Description
User	The name of the user who was logged on when the virus or security risk occurred.
DateFound	The date on which the virus or security risk was found.
EmailSender	The email address that sent the email with the infected attachment.
EmailRecipientList	The list of addresses to which the email with the infected attachment was sent.

Table 26-2 describes the types of information that you can customize for the infection fields.

Table 26-2 Infection information fields

Field	Description
SecurityRiskName	The name of the virus or security risk that was found.
ActionTaken	The action that was taken in response to detecting the virus or security risk. This action can be either the first action or the second action that was configured.
Status	The state of the file: Infected, Not Infected, or Deleted. This message variable is not used by default. To display this information, manually add this variable to the message.
Filename	The name of the file that the virus or the security risk infected.
PathAndFilename	The complete path and name of the file that the virus or security risk infected.
Computer	The name of the computer on which the virus or security risk was found.
User	The name of the user who was logged on when the virus or security risk occurred.
DateFound	The date on which the virus or security risk was found.
OriginalAttachmentName	The name of the attachment that contains the virus or security risk.

Table 26-2 Infection information fields *(continued)*

Field	Description
StorageName	The affected area of the application. For example, the storage name might be File System Auto-Protect or Lotus Notes Auto-Protect.

Displaying Auto-Protect results on infected computers

If you want users to view the results of Auto-Protect scans of files and processes, you can display the results on the infected computers. You can also disable the display if you do not want the results to appear on client computers.

You can click **Help** for more information about the options that are used in the procedures.

To display Auto-Protect results on infected computers

1. On the **Antivirus and Antispyware Policy** page, click **File System Auto-Protect**.
2. On the **Notifications** tab, check or uncheck **Display the Auto-Protect results dialog on the infected computer**.
3. If you are finished configuring policy settings, click **OK**.

Adding warnings to infected email messages

For supported email software, you can configure Auto-Protect to insert a warning automatically into the body of an infected email message. A warning message is important if the Symantec Endpoint Protection client is unable to clean the virus from the message. The message is also important if an infected attachment file is moved, left alone, deleted, or renamed. The warning message tells you which virus was found and explains the action that was taken.

You can append the following text to the top of the email message that is associated with the infected attachment:

Symantec Endpoint Protection found a security risk in an attachment from [EmailSender].

For each infected file, the following information is also added to the email message:

- The name of the file attachment
- The name of the risk
- The action taken

- The infection status of the file

You can customize the subject and body of the message.

The email message contains a field called EmailSender. You can customize the default message.

The message would look as follows to the recipient:

```
Symantec Endpoint Protection found a security risk in an
attachment from John.Smith@mycompany.com.
```

You can click **Help** for more information about the options that are used in the procedures.

To add email warnings to infected email messages

1. On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click one of the following options:
   - **Internet Email Auto-Protect**.
   - **Microsoft Outlook Auto-Protect**.
   - **Lotus Notes Auto-Protect**.
2. On the **Notifications** tab, under **Email Notifications**, check **Insert a warning into the email message**.
3. Click **Warning** and do one of the following actions:
   - Click **OK** to accept the default message.
   - Customize the warning message.
4. If you are finished with the configuration for this policy, click **OK**.

Notifying senders of infected email messages

For supported email software, you can configure Auto-Protect to respond automatically to the sender of an email message that contains an infected attachment.

Note: Use caution when you configure the options to notify senders about infected email messages. The address of the infected email message might be spoofed. If you send notifications, you might generate spam and cause increased traffic on your network.

You can also configure Auto-Protect to send a default reply email message with the following subject:

Security risk found in message "[EmailSubject]"

The body of the message informs the sender of the infected attachment:

Symantec Endpoint Protection found a security risk in an attachment you ([EmailSender]) sent to [EmailRecipientList].

To ensure the recipients are able to use the files you sent, perform a virus scan on your computer, clean any infected files, then resend this attachment.

For each infected file, the following information is also added to the email message:

- The name of the file attachment
- The name of the risk
- The action taken
- The infection status of the file

You can also customize this message.

To notify senders of infected email messages

1. On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click one of the following options:
   - **Internet Email Auto-Protect**.
   - **Microsoft Outlook Auto-Protect**.
   - **Lotus Notes Auto-Protect**.
2. On the **Notifications** tab, under **Email Notifications**, check **Send email to the sender**.
3. Click **Sender**.
4. In the **Send Email to Sender** dialog box, on the **Message** tab, under **Message Text**, do one of the following actions:
   - Click **OK** to accept the default message.
   - Type a subject line, message body, and infection information to appear in each message, and then click **OK**.
     You can click **Help** for information about the variables that you can use in the message.
5. For Internet Email Auto-Protect only, on the **Email Server** tab, type the following information:.
   - The mail server name and port
   - The user name and password

- The reverse path for the email

6 If you are finished with the configuration for this policy, click **OK**.

Notifying others of infected email messages

For supported email software, you can configure Auto-Protect to notify others whenever an email message that contains an infected attachment is opened.

Note: Use caution when you configure the options to notify others about infected email messages. The address of the infected email message might be spoofed. If you send notifications, you might generate spam and cause increased traffic on your network.

You can send an email message to other users with the following subject:

Security risk found in message "[EmailSubject]"

The body of the message includes information about the sender of the infected attachment:

Symantec Endpoint Protection found a security risk in an attachment from [EmailSender].

For each infected file, the following information is also added to the email message:

- The name of the file attachment
- The name of the risk
- The action taken
- The infection status of the file

You can also customize this message.

To notify others of infected email messages

1 On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click one of the following options:

- **Internet Email Auto-Protect**.
- **Microsoft Outlook Auto-Protect**.
- **Lotus Notes Auto-Protect**.

2 On the **Notifications** tab, under **Email Notifications**, check **Send email to others**.

3 Click **Others**.

4 In the **Send Email to Others** dialog box, on the **Others** tab, provide one or more email addresses to which notifications should be sent.

5 Click the **Message** tab and type a subject line, message body, and infection information to appear in each message.

You can click **Help** for information about the variables that you can use in the message.

6 For **Internet Email Auto-Protect** only, on the **Email Server** tab, type the following information:.

- The mail server name and port
- The user name and password
- The reverse path for the email

7 Click **OK**.

8 If you are finished with the configuration for this policy, click **OK**.

Configuring progress notifications for Auto-Protect scans of Internet email

You can enable or disable progress indicator options for Auto-Protect scans of Internet email.

You can configure the following options:

- Whether or not to display a progress window on the client computer when an email message is sent.
- Whether or not to display an icon in the notification area to indicate the transmission status of the email.

Both options are enabled by default.

To configure progress notifications

1 On the **Antivirus and Antispyware Policy** page, under **Windows Settings**, click **Internet Email Auto-Protect**.

2 On the **Notifications** tab, under **Progress Notifications,** check or uncheck the following options:

- **Display a progress indicator when email is being sent**.
- **Display a notification area icon**.

3 If you are finished with the configuration for this policy, click **OK**.

Chapter 27

Using administrator-defined scans

This chapter includes the following topics:

About using administrator-defined scans

Administrator-defined scans include antivirus and antispyware scheduled scans and on-demand scans. You configure options for these types of scans as part of an Antivirus and Antispyware Policy.

You use scheduled scans and on-demand scans to supplement the protection that Auto-Protect provides. Auto-Protect provides protection when you read and write files. Scheduled scans and on-demand scans can scan any files that exist on your

client computers. They can also protect memory, load points, and other important locations on your client computers.

Note: For managed clients, Symantec Endpoint Protection provides a default scheduled scan that scans all files, folders, and locations on the client computers.

Some options for administrator-defined scans are similar to the options for Auto-Protect scans. The similar options include the detection actions and the notifications that you specify.

See "Configuring the options that apply to antivirus and antispyware scans" on page 415.

Configuring a scheduled scan for Windows clients

You configure scheduled scans as part of an Antivirus and Antispyware Policy. The scan settings are different for Windows clients and for Mac clients.

See "Configuring a scheduled scan for Mac clients" on page 449.

You can save your scheduled scan settings as a template. You can use any scan that you save as a template as the basis for a different Antivirus and Antispyware Policy. The scan templates can save you time when you configure multiple Antivirus and Antispyware Policies. A scheduled scan template is included by default in the policy. The default scheduled scan scans all files and directories.

You can click Help for more information about the options that are used in this procedure.

To configure a scheduled scan for Windows clients

1. On the Antivirus and Antispyware Policy page, under **Windows Settings**, click **Administrator-defined Scans**.
2. On the **Scans** tab, under **Scheduled Scans**, click **Add**.
3. In the **Add Scheduled Scan** dialog box, click **Create a new scheduled scan**.
4. Click **OK**.
5. In the **Add Scheduled Scan** dialog box, on the **Scan Details** tab, type a name and description for this scheduled scan.
6. Click **Active Scan**, **Full Scan**, or **Custom Scan**.
7. If you selected Custom, under Scanning, you can specify the folders to scan.
8. Under File types, click **Scan all files** or **Scan only selected extensions**.

   See "Configuring scans of selected file extensions" on page 415.

9 Under Enhance the scan by checking, check or uncheck **Memory**, **Common infection locations**, or **Well-known virus and security risk locations**.

10 Click **Advanced Scanning Options**.

11 Set any of the options for compressed files, storage migration, or performance optimization.

12 Click **OK** to save the advanced scanning options for this scan.

13 On the **Schedule** tab, under **Scanning schedule**, set the frequency and the time at which the scan should run.

14 On the **Actions** tab, set any of the options.

See "Configuring actions for known virus and security risk detections on Windows clients" on page 417.

You can also set remediation options for the scan.

15 On the **Notifications** tab, set any of the options.

See "About notification messages on infected computers" on page 419.

16 If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.

17 Click **OK**.

Configuring a scheduled scan for Mac clients

You configure scheduled scans as part of an Antivirus and Antispyware Policy. The scan settings are different for Windows clients and for Mac clients.

See "Configuring a scheduled scan for Windows clients" on page 448.

You can save your scheduled scan settings as a template. You can use any scan that you save as a template as the basis for a different Antivirus and Antispyware Policy. The scan templates can save you time when you configure multiple Antivirus and Antispyware Policies. A scheduled scan template is included by default in the policy. The default scheduled scan scans all files and directories.

To configure a scheduled scan for Mac clients

1 On the Antivirus and Antispyware Policy page, under **Mac Settings**, click **Administrator-defined Scans**.

2 On the **Scans** tab, under **Scheduled Scans**, click **Add**.

3 In the **Add Scheduled Scan** dialog box, click **Create a new scheduled scan**, and then click **OK**.

4 In the **Add Scheduled Scan** dialog box, on the **Scan Details** tab, type a name and a description for the scan.

5 Under **Scan drives and folders**, specify the items to scan.

6 Move the slider to set the priority of the scan.

Scan priority on Mac clients is equivalent to tuning or performance adjustment on Windows clients. High priority means that the scan runs as fast as possible, but other applications may run more slowly during the scan. Low priority means that other applications run as fast as possible, but the scan may run more slowly. Medium priority balances the speed at which applications and scans run.

7 On the **Schedule** tab, under **Scanning schedule**, set the frequency and the time at which the scan should run.

8 If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.

9 Click **OK**.

Configuring an on-demand scan for Windows clients

You can configure options for the custom scans that you want to run on demand. You run the on-demand scans manually from the Clients page. You can also run the on-demand scans from the Monitors page in the management console.

You cannot configure a scan name or a description for the scan options. The client uses the options whenever you run a custom on-demand scan from the management console on the client computer.

Note: You can run an active scan or a full scan on demand.

See "About administrator-defined scans" on page 401.

The settings for on-demand scans are similar to the settings for scheduled scans.

See "Configuring a scheduled scan for Windows clients" on page 448.

You create different scan settings for Windows clients and for Mac clients.

See "Configuring an on-demand scan for Mac clients" on page 451.

You can click Help for more information about the options that are used in this procedure.

To configure settings for on-demand scans for Windows clients

1. On the Antivirus and Antispyware Policy page, under **Windows Settings**, click **Administrator-defined Scans**.
2. On the Scans tab, under Administrator On-demand Scan, click **Edit**.
3. In the Edit Administrator On-demand Scan dialog box, on the Scan Details tab, under Scanning, click **Edit Folders**.

   By default, the scan includes all folders.
4. In the Edit Folders dialog box, select the desired folders, and then click **OK**.
5. In the Edit Administrator On-demand Scan dialog box, under File types, click **Scan all files** or **Scan only selected extensions**.

   See "About scanning selected extensions or folders" on page 403.
6. Under Enhance the scan by checking, check or uncheck **Memory**, **Common infection locations,** or **Well-known virus and security risk locations**.
7. Click **Advanced Scanning Options**.
8. Set any of the options for compressed files, storage migration, or performance optimization.
9. Click **OK** to save the advanced options for this scan.
10. On the Actions tab, set any of the options.

    See "Configuring actions for known virus and security risk detections on Windows clients" on page 417.

    You can also set remediation options for the scan.
11. On the Notifications tab, set any of the options.

    See "About notification messages on infected computers" on page 419.
12. Click **OK**.

Configuring an on-demand scan for Mac clients

You can configure options for the custom scans that you want to run on demand. You run the on-demand scans manually from the Clients page. You can also run the on-demand scans from the Monitors page in the management console.

Whenever you run an on-demand scan on Mac clients, you run a custom scan. The active scan and full scan options are available only for Windows clients.

The settings for on-demand scans are similar to the settings for scheduled scans. You cannot configure a scan name or a description for an on-demand scan, however.

See "Configuring a scheduled scan for Mac clients" on page 449.

You create different scan settings for Windows clients and for Mac clients.

See "Configuring an on-demand scan for Windows clients" on page 450.

You can click Help for more information about the options that are used in this procedure.

Warning: If you do not choose **Automatically repair infected files**, any infected files are not moved to the Quarantine, even if you choose **Quarantine the files that cannot be repaired**.

The software asks whether you want to repair an infected file. If you do not repair the file, it is left on the computer. If you choose **Automatically repair infected files**, and if you do not choose **Quarantine the files that cannot be repaired**, any infected files are deleted.

To configure an on-demand scan for Mac clients

1. On the Antivirus and Antispyware Policy page, under **Mac Settings**, click **Administrator-defined Scans**.
2. On the **Scans** tab, under **Administrator On-demand Scan**, click **Edit**.
3. On the **Scan Details** tab, under **Scan drives and folders**, select the items that you want to include in this scan.
4. Under **Actions**, check or uncheck the following options.

Automatically repair infected files	Symantec Endpoint Protection automatically tries to repair the infected file when a risk is found. If you do not choose this option, any repair must be performed manually.
Quarantine files that cannot be repaired	Symantec Endpoint Protection automatically moves any file that cannot be repaired to the Quarantine.

5. On the **Notifications** tab, set any of the options, and then click **OK**.

   See "About notification messages on infected computers" on page 419.

Running on-demand scans

You can run a manual, or on-demand, scan remotely from the management console in either of the following ways:

- From the **Clients** tab
- From the computer status logs that you generate on the **Monitors** tab
  See "Running commands and actions from logs" on page 274.

For Windows client computers, you can run an active, full, or custom on-demand scan.

By default, the following items are included in the scan:

- All directories
- All file types
- Memory
- Common infection locations
- Well-known virus and security risk locations

For Mac client computers, you can run only a custom on-demand scan.

The custom scan uses the settings that are configured for on-demand scans in the Antivirus and Antispyware Policy.

See "Configuring an on-demand scan for Windows clients" on page 450.

See "Configuring an on-demand scan for Mac clients" on page 451.

You can click Help for more information about the options that are used in the procedures.

Note: If you issue a restart command on a client computer that runs an on-demand scan, the scan stops, and the client computer restarts. The scan does not restart.

To run an on-demand scan on a group

1. In the console, click **Clients**.
2. Under **View Clients**, right-click the group that includes the computers that you want to scan.
3. Click **Run Command on Group > Scan**.
4. In the **Select Scan Type** dialog box, select **Active Scan**, **Full Scan**, or **Custom Scan**.
5. Click **OK**.

6 In the message that appears, click **Yes**.

7 In the confirmation message that appears, click **OK**.

To run an on-demand scan on a computer or user

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

2 In the right pane, under **Clients**, select the computers and users for which you want to run a scan.

3 Right-click the selection, and then click **Run Command on Clients > Scan**.

4 In the message that appears, click **Yes**.

5 In the **Select Scan Type** dialog box, select **Active Scan**, **Full Scan**, or **Custom Scan**.

6 Click **OK**.

7 In the confirmation message that appears, click **OK**.

Configuring scan progress options for administrator-defined scans

You can configure whether or not the Scan Results dialog box appears on client computers. If you allow the dialog box to appear on client computers, users are always allowed to pause or delay an administrator-defined scan.

You can allow users to stop a scan entirely. You can also configure options for how users pause or delay scans.

You can allow the user to perform the following scan actions:

Pause	When a user pauses a scan, the Scan Results dialog box remains open and waits for the user to either continue or abort the scan. If the computer is turned off, the paused scan does not continue.
Snooze	When a user snoozes a scheduled scan, the user has the option of snoozing the scan for one hour or three hours. The number of snoozes is configurable. When a scan snoozes, the Scan Results dialog box closes; it reappears when the snooze period ends and the scan resumes.
Stop	When a user stops a scan, the scan usually stops immediately. If a user stops a scan while the client software scans a compressed file, the scan does not stop immediately. In this case, the scan stops as soon as the compressed file has been scanned. A stopped scan does not restart.

A paused scan automatically restarts after a specified time interval elapses.

You can click Help for more information about the options that are used in this procedure.

To configure scan progress options for administrator-defined scans

1. On the Antivirus and Antispyware Policy page, click **Administrator-defined Scans**.
2. On the Advanced tab, under Scan Progress Options, click **Show scan progress** or **Show scan progress if risk detected**.
3. To automatically close the scan progress indicator after the scan completes, check **Close the scan progress window when done**.
4. Check **Allow user to stop scan**.
5. Click **Pause Options**.
6. In the Scan Pause Options dialog box, do any of the following actions:
   - To limit the time that a user may pause a scan, check **Limit the time the scan may be paused**, and then type a number of minutes. The range is 3 to 180.
   - To limit the number of times a user may delay (or snooze) a scan, in the Maximum number of snooze opportunities box, type a number between 1 and 8.
   - By default, a user can delay a scan for 1 hour. To change this limit to 3 hours, check **Allow users to snooze the scan for 3 hours**.
7. Click **OK**.

Setting advanced options for administrator-defined scans

You can set advanced options for scheduled scans and on-demand scans.

You can click Help for more information about the options that are used in the procedure.

To set advanced options for administrator-defined scans

1. On the Antivirus and Antispyware Policy page, click **Administrator-defined Scans**.
2. On the Advanced tab, under Scheduled Scans, check or uncheck the following options:
   - **Delay scheduled scans when running on batteries**

- **Allow user-defined scheduled scans to run when scan author is not logged on**
- **Display notifications about detections when the user logs on**

3 Under **Startup and Triggered Scans**, check or uncheck the following options:

- **Run startup scans when users log on**
- **Allow users to modify startup scans**
- **Run an Active Scan when new definitions arrive**

4 Click **OK**.

Section 4

Configuring Network Threat Protection

Chapter 28

Basic Network Threat Protection settings

This chapter includes the following topics:

About Network Threat Protection and network attacks

Network attacks take advantage of the way that computers transfer information. The client can protect computers by monitoring the information that comes into and out of the computer, and by blocking attack attempts.

Information travels across the Internet in the form of packets. Each packet includes a header that contains information about the sending computer, the intended recipient, how the data in the packet should be processed, and the port that should receive the packet.

Ports are the channels that divide the stream of information that comes from the Internet into separate paths that individual applications handle. When Internet applications run on a computer, they listen to one or more ports and accept the information that is sent to these ports.

Network attacks take advantage of weaknesses in specific Internet programs. Attackers use the tools that send the packets that contain malicious programming code to a particular port. If an application that is vulnerable to this attack listens to that port, the code can let the attacker gain access to, disable, or even take control of the computer. The programming code that is used to generate the attacks may be contained inside of a single packet or span several packets.

You can install the client with default settings for Network Threat Protection. In most cases you do not have to change the settings. It is generally safe to leave the settings as they are. However, if you have a detailed understanding of networks, you can make many changes in the client firewall to fine-tune the client computer's protection.

See "How Symantec Endpoint Protection protects computers against network attacks" on page 460.

How Symantec Endpoint Protection protects computers against network attacks

The Symantec Endpoint Protection client includes the following tools that protect computers in your organization from intrusion attempts:

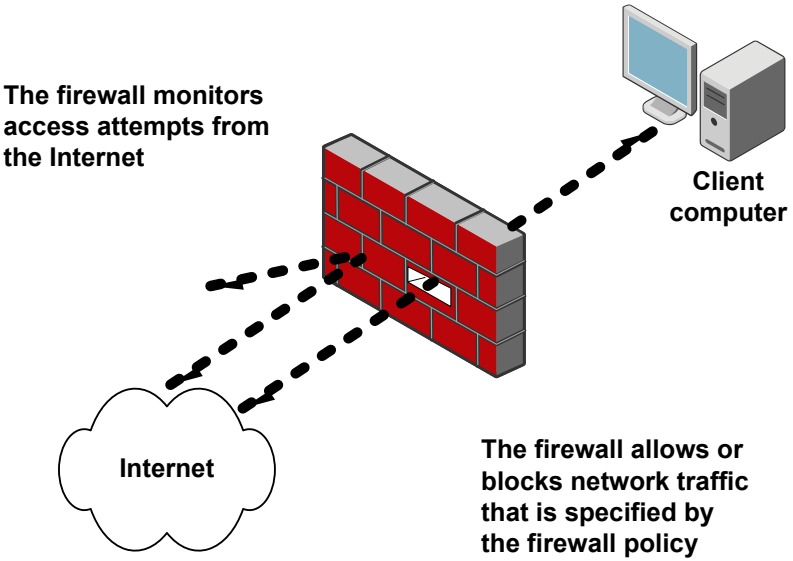
Firewall	Monitors all Internet communication and creates a shield that blocks or limits the attempts to view information on the computer. See "About the firewall" on page 461.

Intrusion prevention	Analyzes all inbound information and outbound information for the data patterns that are typical of an attack. See "About the intrusion prevention system" on page 483.

About the firewall

The Symantec Endpoint Protection firewall is software that provides a barrier between the computer and the Internet. The firewall prevents unauthorized users from accessing the computers and the networks that connect to the Internet. It detects possible hacker attacks, protects personal information, and eliminates unwanted sources of network traffic.

Figure 28-1 Information flow on a network when a computer has a firewall



All the information that enters or leaves the private network must pass through the firewall, which examines the information packets. The firewall blocks the packets that do not meet the specified security criteria. The way the firewall examines the information packets is through the use of a Firewall Policy. Firewall Policies consist of one or more rules that work together to allow or block users from accessing the network. Only authorized traffic can pass. The Firewall Policy defines the authorized traffic.

The firewall works in the background. You determine the level of interaction that you want users to have with the client by permitting or blocking their ability to

configure firewall rules and firewall settings. Users might interact with the client only when it notifies them of new network connections and possible problems, or they might have full access to the user interface.

See "About firewall rules" on page 463.

See "About working with Firewall Policies" on page 462.

About working with Firewall Policies

The Symantec Endpoint Protection Manager includes a default Firewall Policy with firewall rules and firewall settings for the office environment. The office environment is normally under the protection of corporate firewalls, boundary packet filters, or antivirus servers. Therefore, it is normally more secure than most home environments, where limited boundary protection is available.

When you install the console for the first time, it adds a default Firewall Policy to each group automatically. Every time you add a new location, the console copies a Firewall Policy to the default location automatically.

If the default protection is not appropriate, you can customize the Firewall Policy for each location, such as for a home site or customer site. If you do not want the default Firewall Policy, you can edit it or replace it with another shared policy.

Firewall Policies include the following elements:

Firewall rules	Firewall rules are policy components that control how the firewall protects computers from malicious incoming traffic and applications. The firewall automatically checks all incoming and outgoing packets against these rules, and allows or blocks the packets based on information specified in rules. See "About firewall rules" on page 463.
Smart traffic filters	Allows the specific types of traffic that are required on most networks such as DHCP, DNS, and WINS traffic. See "Enabling Smart traffic filtering" on page 479.
Traffic and stealth settings	Detects and blocks traffic that comes from certain drivers, protocols, and other sources. See "Enabling traffic and stealth settings" on page 480.
Peer-to-peer authentication settings	Blocks a remote computer from connecting to a client computer until the client computer has authenticated that remote computer. See "Configuring peer-to-peer authentication" on page 481.

You can set a location to client control or mixed control so that the user can customize the Firewall Policy.

See "Configuring Network Threat Protection settings for mixed control" on page 499.

You create and edit Firewall Policies similarly to the way you create and modify other types of policies. You can assign, withdraw, replace, copy, export, import, or delete a Firewall Policy.

You typically assign a policy to multiple groups in your security network. You can create a non-shared, location-specific policy if you have specific requirements for a particular location.

You should be familiar with the basics of policy configuration to work with policies.

See "Using policies to manage your network security" on page 90.

About firewall rules

Firewall rules control how the client protects the client computer from malicious inbound traffic and malicious outbound traffic. The firewall automatically checks all the inbound and the outbound packets against these rules. The firewall then allows or blocks the packets based on the information that is specified in rules. When a computer tries to connect to another computer, the firewall compares the type of connection with its list of firewall rules.

See "About the elements of a firewall rule" on page 463.

See "About the rule processing order" on page 468.

See "About stateful inspection" on page 471.

About the elements of a firewall rule

In general, a firewall rule describes the conditions in which a network connection may be allowed or denied. You use the following criteria to define a firewall rule:

Triggers	Applications, hosts, protocols, and network adapters When the firewall evaluates the rule, all the triggers must be true for a positive match to occur. If any one trigger is not true in relation to the current packet, the firewall cannot apply the rule. You can combine the trigger definitions to form more complex rules, such as to identify a particular protocol in relation to a specific destination address. See "About application triggers" on page 464. See "About host triggers" on page 465. See "About network service triggers" on page 467. See "About network adapter triggers" on page 468.
Conditions	Schedule and screen saver state The conditional parameters do not describe an aspect of a network connection. Instead, the conditional parameters determine the active state of a rule. You may define a schedule or identify a screen saver state that dictates when a rule is considered to be active or inactive. The conditional parameters are optional and if not defined, not significant. The firewall does not evaluate inactive rules.
Actions	Allow or block, and log or do not log The action parameters specify what actions the firewall takes when it successfully matches a rule. If the rule matches and is selected in response to a received packet, the firewall performs all actions. The firewall either allows or blocks the packet and logs or does not log the packet. If the firewall allows traffic, it lets the traffic that the rule specifies access the network. If the firewall blocks traffic, it blocks the traffic that the rule specifies so that it does not access the network.

A rule that combines all criteria might allow traffic to IP address 192.58.74.0 on remote port 80 between 9 AM and 5 PM daily.

See "About firewall rules" on page 463.

About application triggers

When the application is the only trigger you define in a rule that allows traffic, the firewall allows the application to perform any network operation. The application is the significant value, not the network operations that the application performs. For example, suppose you allow Internet Explorer and you define no other triggers. 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 particular network protocols and hosts with which communication is allowed.

Application-based rules may be difficult to troubleshoot because an application may use multiple protocols. For example, if the firewall processes a rule that allows Internet Explorer before a rule that blocks FTP, the user can still communicate with FTP. The user can enter an FTP-based URL in the browser, such as ftp://ftp.symantec.com.

You should not use application rules to control traffic at the network level. For example, a rule that blocks or limits the use of Internet Explorer would have no effect should the user use a different Web browser. The traffic that the other Web browser generates would be compared against all other rules except the Internet Explorer rule. Application-based rules are more effective when the rules are configured to block the applications that send and receive traffic.

Note: If Trend Micro PC-cillin IS 2007 and the Symantec Endpoint Protection client are installed on the same computer, firewall rules for a specific Web browser do not work. Trend Micro PC-cillin delivers Web traffic to its own proxy software. In Trend Micro PC-cillin, you must disable the Web site access controls and data threat prevention option.

See "About the elements of a firewall rule" on page 463.

About host triggers

When you define host triggers, you specify the host on both sides of the described network connection.

Traditionally, the way to express the relationship between hosts is referred to as being either the source or destination of a network connection.

You can define the host relationship in either one of the following ways:

Source and destination	The source host and destination host is dependent on the direction of traffic. In one case the local client computer might be the source, whereas in another case the remote computer might be the source. The source and the destination relationship is more commonly used in network-based firewalls.
Local and remote	The local host is always the local client computer, and the remote host is always a remote computer that is positioned elsewhere on the network. This expression of the host relationship is independent of the direction of traffic. The local and the remote relationship is more commonly used in host-based firewalls, and is a simpler way to look at traffic.

Figure 28-2 illustrates the source and destination relationship with respect to the direction of traffic.

Figure 28-2 The relationship between source and destination hosts

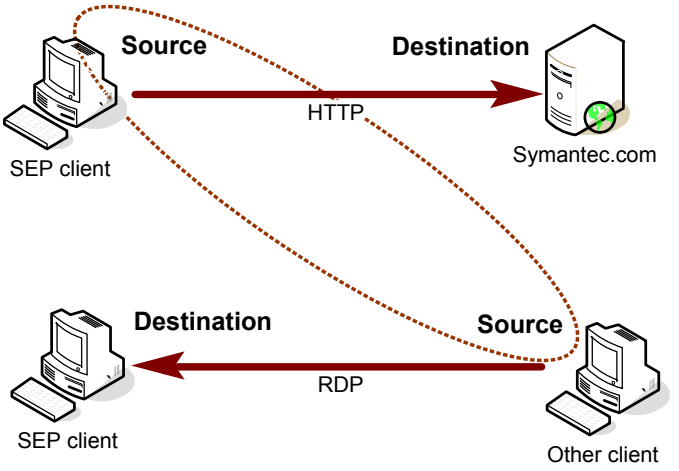
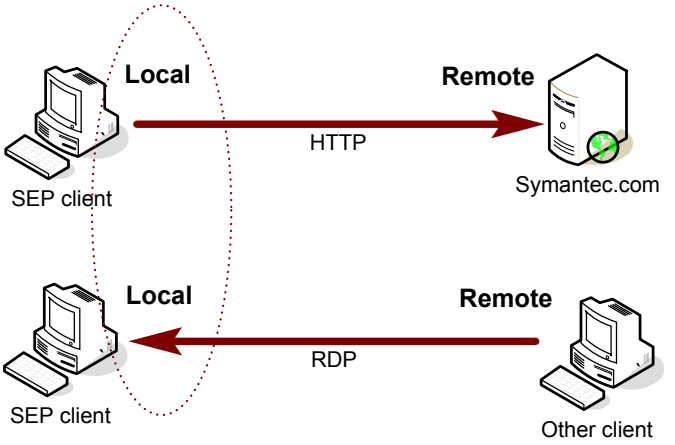


Figure 28-3 illustrates the local host and remote host relationship with respect to the direction of traffic.

Figure 28-3 The relationship between local and remote hosts



You can define multiple source hosts and multiple destination hosts. The hosts that you define on either side of the connection are evaluated by using an OR

statement. The relationship between the selected hosts is evaluated by using an AND statement.

For example, consider a rule that defines a single local host and multiple remote hosts. As the firewall examines the packets, the local host must match the relevant IP address. However, the opposing sides of the address may be matched to any remote host. For example, you can define a rule to allow HTTP communication between the local host and either symantec.com, yahoo.com, or google.com. The single rule is the same as three rules.

See "Adding hosts and host groups to a rule" on page 502.

See "About the elements of a firewall rule" on page 463.

About network service triggers

A network service trigger identifies one or more network protocols that are significant in relation to the described network traffic.

You can define the following types of protocols:

TCP	Port or port ranges
UDP	Port or port ranges
ICMP	Type and code
IP	Protocol number (IP type) Examples: Type 1 = ICMP, Type 6 = TCP, Type 17 = UDP
Ethernet	Ethernet frame type Examples: Type 0x0800 = IPv4, Type = 0x8BDD = IPv6, Type 0x8137 = IPX

When you define TCP-based or UDP-based service triggers, you identify the ports on both sides of the described network connection. Traditionally, ports are referred to as being either the source or the destination of a network connection.

You can define the network service relationship in either of the following ways:

Source and destination	The source port and destination port are dependent on the direction of traffic. In one case the local client computer might own the source port, whereas in another case the remote computer might own the source port.
Local and remote	The local host computer always owns the local port, and the remote computer always owns the remote port. This expression of the port relationship is independent of the direction of traffic.

You specify the direction of traffic when you define the protocol.

You can define multiple protocols. For example, a rule might include the ICMP, IP, and TCP protocols. The rule describes multiple types of connections that may occur between the identified client computers, or are used by an application.

See "About the elements of a firewall rule" on page 463.

About network adapter triggers

When you define a network adapter trigger, the rule is relevant only to the traffic that is transmitted or received by using the specified type of adapter.

You can specify one of the following types of adapters:

- Ethernet
- Wireless
- Dial-up
- Any VPN
- Vender-specific virtual adapters

When you define a particular type of adapter, consider how that adapter is used. For example, if a rule allows outbound HTTP traffic from Ethernet adapters, then HTTP is allowed through all the installed adapters of the same type. The only exception is if you also specify local host addresses. The client computer may use multi-NIC servers and the workstations that bridge two or more network segments. To control traffic relative to a particular adapter, the address scheme of each segment must be used rather than the adapter itself.

See "About the elements of a firewall rule" on page 463.

About the rule processing order

Firewall rules are ordered sequentially, from highest to lowest priority, or from the top to bottom in the Rules list. The firewall inspects the rules in this order. If the first rule does not specify how to handle a packet, the firewall inspects the second rule for information on how to handle a packet. This process continues until the firewall finds a match. After the firewall finds a match, the firewall takes the action that the rule specifies, and subsequent lower priority rules are not inspected. For example, if a rule that blocks all traffic is listed first, followed by a rule that allows all traffic, the client blocks all traffic.

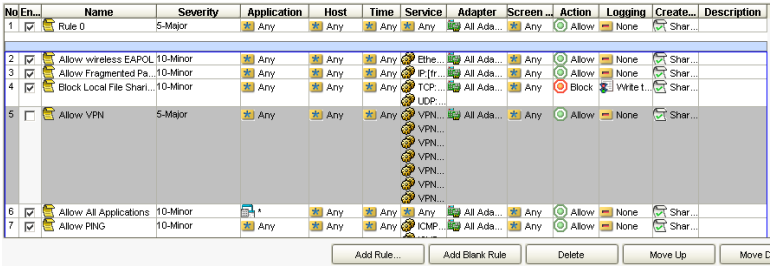
Table 28-1 Sequence for processing firewall rules, IPS signatures, and settings

Priority	Setting
First	Custom IPS signatures
Second	Intrusion prevention settings, traffic settings, and stealth settings
Third	Smart traffic filters
Fourth	Firewall rules
Fifth	Port scan checking
Sixth	IPS signatures that are downloaded through LiveUpdate

The Rules list contains a blue dividing line. The dividing line sets the priority of rules in the following situations:

- When a subgroup inherits rules from a parent group.
- When the client is set to mixed control. The firewall processes both server rules and client rules.

Figure 28-4 Rules list



See "About firewall rules" on page 463.

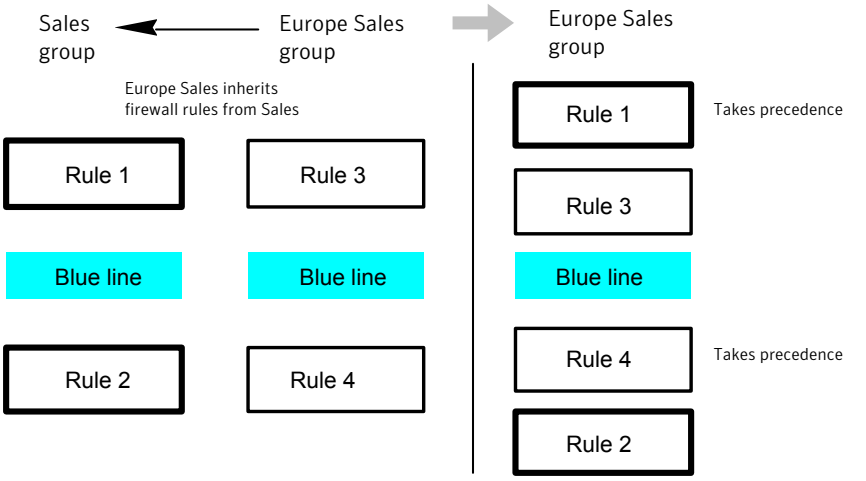
About inherited rules

The firewall processes inherited firewall rules in the Rules list as follows:

- Above the blue dividing line, the rules that the policy inherits take precedence over the rules that you create.
- Under the blue dividing line, the rules that you create take precedence over the rules that the policy inherits.

Figure 28-5 displays how the Rules list orders rules when a subgroup inherits rules from a parent group. In this example, the Sales group is the parent group. The Europe Sales group inherits from the Sales group.

Figure 28-5 An example of how firewall rules inherit from each other



See "Adding inherited rules from a parent group" on page 476.

About server rules and client rules

Rules are categorized as either server rules or client rules. Server rules are the rules that you create in Symantec Endpoint Protection Manager and that are downloaded to the Symantec Endpoint Protection client. Client rules are the rules that the user creates on the client.

Table 28-2 describes the relationship between the client's user control level and the user's interaction with the firewall rules.

Table 28-2 User control level and rule status

User control level	User interaction
Server control	The client receives server rules but the user cannot view them. The user cannot create client rules.
Mixed control	The client receives server rules. The user can create client rules, which are merged with server rules and client security settings.
Client control	The client does not receive server rules. The user can create client rules. You cannot view client rules.

See "Configuring user interface settings" on page 168.

For clients in mixed control, the firewall processes server rules and client rules in a particular order.

Table 28-3 lists the order that the firewall processes server rules and client rules and client settings.

Table 28-3 Server rules and client rules processing priority

Priority	Rule type or setting
First	Server rules with high priority levels (rules above the blue line in the Rules list)
Second	Client rules
Third	Server rules with lower priority levels (rules under the blue line in the Rules list) On the client, server rules under the blue line are processed after client rules.
Fourth	Client security settings
Fifth	Client application-specific settings

On the client, users can modify a client rule or security setting, but users cannot modify a server rule.

Warning: If the client is in mixed control, users can create a client rule that allows all traffic. This rule overrides all server rules under the blue line.

See "Changing the order of rules" on page 478.

About stateful inspection

The firewall uses stateful inspection, a process that tracks information about current connections such as source and destination IP addresses, ports, and applications. The client makes traffic flow decisions by using this connection information before it inspects firewall rules.

For example, if a firewall rule permits a client 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 client is expected, and permits the Web server traffic to flow to the initiating client without inspecting the rulebase. A rule must permit the initial outbound traffic before the firewall logs the connection.

Stateful inspection lets you simplify rulebases because you do not have to create the rules that permit traffic in both directions for traffic that is typically initiated in one direction only. Client traffic that is typically initiated in one direction includes Telnet (port 23), HTTP (port 80), and HTTPS (port 443). Clients initiate this traffic outbound, so you only have to create a rule that permits outbound traffic for these protocols. The firewall permits the return traffic.

By configuring only outbound rules, you increase client security in the following ways:

- Reduce rulebase complexity.
- Eliminate the possibility that a worm or other malicious program can initiate connections to a client on the ports that are configured for outbound traffic only. You can also configure inbound rules only, for traffic to clients that clients do not initiate.

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 when necessary. For example, for clients to use the ping command and receive replies, you must create a rule that permits ICMP traffic in both directions.

Because the firewall is stateful in nature, you only need to create rules that initiate a connection, not the characteristics of a particular packet. All packets belonging to an allowed connection are implicitly allowed as being an integral part of that same connection.

See "About firewall rules" on page 463.

About UDP connections

For UDP communications, the client analyzes the first UDP datagram and applies the action that is taken on the initial datagram to all subsequent UDP datagrams for the current program session. Inbound or outbound traffic between the same computers is considered part of the UDP connection.

For stateful UDP traffic, when a UDP connection is made, the inbound UDP communication is allowed, even if the firewall rule blocks it. For example, if a rule blocks inbound UDP communications for a specific application, but you choose to allow an outbound UDP datagram, all inbound UDP communications are allowed for the current application session. For stateless UDP, you must create a firewall rule to allow the inbound UDP communication response.

A UDP session times out after 40 seconds if the application closes the port.

Adding blank rules

When you create a new Firewall Policy, the policy includes several default rules. The default rules give you basic protection for an office environment. If you need additional firewall rules, you can add them.

You add rules in the following ways:

- Add a blank rule to the list and then manually configure it.
- Run the Firewall Rule Wizard.
  See "Adding rules with a wizard" on page 475.

To simplify rulebase management, you must specify both the inbound and the outbound traffic in the rule whenever possible. You do not need to create inbound rules for traffic such as HTTP. The Symantec Endpoint Protection client uses stateful inspection for TCP traffic and does not need a rule to filter the return traffic that the clients initiate.

See "About stateful inspection" on page 471.

To add blank rules

1. In the console, open a Firewall Policy.

   See "Editing a policy" on page 97.
2. On the Firewall Policy page, click **Rules**.
3. On the Rules tab, under the Rules list, click **Add Blank Rule**.
4. In the **Name** text box, type a name for the rule.
5. In the Severity field, click the drop-down list and select one of the following options:
   - Critical
   - Major
   - Minor
   - Information
6. Right-click the **Application** field, click **Edit**, and in the Application List dialog box, define an application.

   See "Adding applications to a rule" on page 509.
7. Click **OK**, and then click **OK** again.
8. Right-click the **Host** field, click **Edit**, and in the Host list, define a host.

   See "Adding hosts and host groups to a rule" on page 502.

9 Click **OK**, and then click **OK** again.

10 Right-click the **Time** field, click **Edit**, and then set up a schedule.

See "Adding schedules to a rule" on page 510.

11 Click **OK**, and then click **OK** again.

12 Right-click the **Service** field, and then click **Edit** to add or configure a custom network service.

See "Adding network services to a rule" on page 504.

13 Click **OK**.

14 Right-click the **Adapter** field and select one or more of the following items:

- All Adapters
- Any VPN
- Dial-up
- Ethernet
- Wireless
- More Adapters
  You can add and select from a list of vendor-specific adapters

See "Adding network adapters" on page 507.

15 Right-click the **Screen Saver** field and select which state you want the screen saver to be in:

- On
- Off
- Any

16 Right-click the **Action** field and select the action you want the firewall to take when the traffic matches rule:

- Allow
- Block
- Ask

17 Right-click the **Logging** field and select one or more logging actions you want the firewall to take when the traffic matches the rule:

- Write to Traffic Log
- Write to Packet Log

- Send Email Alert
  See "Configuring email messages for traffic events" on page 513.

The Created At field is not editable. If the policy is shared, the field displays the term Shared. If the policy is not shared, the field displays the name of the group that the non-shared policy is assigned to.

18 Right-click the **Description** field, and then click **Edit**.

19 In the Enter Description dialog box, type an optional description for the rule, and then click **OK**.

20 When you are finished adding the rule, do one of the following actions:

- Add another rule.
- Add Smart traffic filtering settings or traffic and stealth settings.
  See "Enabling Smart traffic filtering" on page 479.
  See "Enabling traffic and stealth settings" on page 480.
- If you are done with the configuration of the policy, click **OK**.

21 If you are prompted, assign the policy to a location.

See "Assigning a shared policy" on page 98.

Adding rules with a wizard

Use the Add Firewall Rule Wizard to create one of the following types of rules:

Application rules	A rule that is based on a specific running process that attempts to use network resources
Host rules	A rule that is based on the endpoints of network connections
Service rules	A rule that is based on the protocols that are used by network connections

You may need to include two or more criteria to describe specific network traffic, such as a particular protocol that originates from a specific host. You must configure the rule after you add it, because the Add Firewall Rule Wizard does not configure new rules with multiple criteria.

When you become familiar with how rules are defined and processed, you may want to add blank rules and configure the various fields as needed. A blank rule allows all traffic.

See "Adding blank rules" on page 473.

To add rules with a wizard

1. In the console, open a Firewall Policy.

   See "Editing a policy" on page 97.

2. On the Firewall Policy page, click **Rules**.
3. On the Rules tab, under the Rules list, click **Add Rule**.
4. In the Add Firewall Rule Wizard, click **Next**.
5. In the Select Rule Type panel, select one of the types of rules.
6. Click **Next**.
7. Enter data on each panel to create the type of rule you selected.
8. For applications and hosts, click **Add More** to add additional applications and services.
9. When you are done, click **Finish**.
10. In the Rules list, right-click any field to edit the rule.
11. When you are finished with the configuration of this policy, click **OK**.

Adding inherited rules from a parent group

You can add rules by inheriting only the rules from a parent group. To inherit the rules from a parent group, the subgroup's policy must be a non-shared policy.

Note: If the group inherits all of its policies from a parent group, this option is unavailable.

Inherited rules are automatically enabled. The subgroup's policy can inherit only the firewall rules that are enabled in the parent group. When you have inherited the rules, you can disable them, but you cannot modify them. As the new rules are added to the parent group's policy, the new rules are automatically added to the inheriting policy.

When the inherited rules appear in the Rules list, they are shaded in purple. Above the blue line, the inherited rules are added above the rules that you created. Below the blue line, the inherited rules are added below the rules that you created.

A Firewall Policy also inherits default rules, so the subgroup's Firewall Policy may have two sets of default rules. You may want to delete one set of default rules.

If you want to remove the inherited rules, you uninherit them rather than delete them. You have to remove all the inherited rules rather than the selected rules.

To add inherited rules from a parent group

1 In the console, open a Firewall Policy.

See "Editing a policy" on page 97.

2 On the Firewall Policy page, click **Rules**.

3 On the Rules tab, above the Rules list, check **Inherit Firewall Rules from Parent Group**.

To remove the inherited rules, uncheck **Inherit Firewall Rules from Parent Group**.

4 Click **OK**.

Importing and exporting rules

You can export and import firewall rules and settings from another Firewall Policy so that you do not have to re-create them. For example, you can import a partial rule set from one policy into another. To import rules, you first have to export the rules to a .dat file and have access to the file.

The rules are added in the same order that they are listed in the parent policy with respect to the blue line. You can then change their processing order.

To export rules

1 In the console, open a Firewall Policy.

See "Editing a policy" on page 97.

2 On the Firewall Policy page, click **Rules**.

3 In the Rules list, select the rules you want to export, right-click, and then click **Export**.

4 In the Export Policy dialog box, locate a directory to save the .dat file, type a file name, and then click **Export**.

To import rules

1 In the console, open a Firewall Policy.

See "Editing a policy" on page 97.

2 On the Firewall Policy page, click **Rules**.

3 Right-click the Rules list, and then click **Import**.

4 In the Import Policy dialog box, locate the .dat file that contains the firewall rules to import, and then click **Import**.

5 In the Input dialog box, type a new name for the policy, and then click **OK**.

6 Click **OK**.

Copying and pasting rules

You can copy and paste rules from the same policy or another policy.

To copy and paste rules

1 In the console, open a Firewall Policy.

See "Editing a policy" on page 97.

2 In the Firewall Policy page, click **Rules**.

3 On the Rules tab, right-click the rule you want to copy, and then click **Copy Rule**.

4 Right-click the row where you want the rule to be pasted, and then click **Paste Rule**.

5 Click **OK**.

Changing the order of rules

The firewall processes the list of firewall rules from the top down. You can determine how the firewall processes firewall rules by changing their order. When you change the order, it affects the order for the currently selected location only.

To change the order of rules

1 In the console, open a Firewall Policy.

See "Editing a policy" on page 97.

2 In the Firewall Policy page, click **Rules**, and then select the rule that you want to move.

3 Do one of the following tasks:

- To process this rule before the previous rule, click **Move Up**.
- To process this rule after the rule below it, click **Move Down**.

4 Click **OK**.

Enabling and disabling rules

Rules must be enabled for the firewall to process them. You can disable a firewall rule if you need to allow specific access to a computer or application. The rule is disabled for the all locations if it is a shared policy, and only one location if it is a location-specific policy. The rule is also disabled for all inherited policies.

To enable and disable rules

1. In the console, open a Firewall Policy.

   See "Editing a policy" on page 97.

2. In the Firewall Policy page, click **Rules**.
3. On the Rules tab, select the rule you want to enable or disable, and then check or uncheck the check box in the Enabled column.
4. Click **OK**.

Enabling Smart traffic filtering

Smart traffic filters allow communication between certain network services so that you do not have to define the rules that explicitly allow those services. The Smart traffic filters allow outbound requests and inbound replies for the network connections that have been configured to use DHCP, DNS, and WINS traffic.

The filters allow DHCP, DNS, or WINS clients to receive an IP address from a server while protecting the clients against attacks from the network.

- If the client sends a request to the server, the client waits for five seconds to allow an inbound response.
- If the client does not send a request to the server, each filter does not allow the packet.

Smart filters allow the packet if a request was made. They do not block packets. The firewall rules allow or block packets.

Note: To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

See "About mixed control" on page 167.

To enable Smart traffic filtering

1. In the console, open a Firewall Policy.

   See "Editing a policy" on page 97.

2. In the Firewall Policy page, click **Smart Traffic Filtering**.
3. If not checked already, check any of the following check boxes:
   - **Enable Smart DHCP**
   - **Enable Smart DNS**
   - **Enable Smart WINS**

   For more information on these options, click **Help**.
4. Click **OK**.
5. If you are prompted, assign the policy to a location.

   See "Assigning a shared policy" on page 98.

Enabling traffic and stealth settings

You can enable various traffic settings and stealth Web browsing settings to protect against certain types of network attacks on the client. You can enable traffic settings to detect and block the traffic that communicates through drivers, NetBIOS, and token rings. You can also configure settings to detect the traffic that uses more invisible attacks. You can also control the behavior for the IP traffic that does not match any firewall rules. After the firewall has completed certain operations, control is passed to a number of components. Each component is designed to perform a different type of packet analysis.

Note: To configure these settings in mixed control, you must also enable these settings in the Client User Interface Mixed Control Settings dialog box.

See "About mixed control" on page 167.

To enable traffic and stealth settings

1. In the console, open a Firewall Policy.

   See "Editing a policy" on page 97.

2. In the Firewall Policy page, click **Traffic and Stealth settings**.
3. If a check box is not checked already, check any one of the check boxes in the Traffic Settings group box and Stealth Settings group box.

   For more information on these options, click **Help**.

4 Click **OK**.

5 If you are prompted, assign the policy to a location.

See "Assigning a shared policy" on page 98.

Configuring peer-to-peer authentication

You can use peer-to-peer authentication to allow a remote client computer (peer) to connect to another client computer (authenticator) within the same corporate network. The authenticator temporarily blocks inbound TCP and UDP traffic from the remote computer until the remote computer passes the Host Integrity check.

The Host Integrity check verifies the following characteristics of the remote computer:

- The remote computer has both Symantec Endpoint Protection and Symantec Network Access Control installed.
- The remote computer meets the Host Integrity Policy requirements.

If the remote computer passes the Host Integrity check, the authenticator allows the remote computer to connect to it.

If the remote computer fails the Host Integrity check, the authenticator continues to block the remote computer. You can specify how long the remote computer is blocked before it can try to connect to the authenticator again. You can also specify certain remote computers to always be allowed, even if they would not pass the Host Integrity check. If you do not enable a Host Integrity Policy for the remote computer, the remote computer passes the Host Integrity check.

Peer-to-peer authentication information is displayed in the Compliance Enforcer Client log and in the Network Threat Protection Traffic log.

Note: Peer-to-peer authentication works in server control and mixed control, but not in client control.

Warning: Do not enable peer-to-peer authentication for the clients that are installed on the same computer as the management server. Otherwise, the management server cannot download policies to the remote computer if the remote computer fails the Host Integrity check.

To configure peer-to-peer authentication

1. In the console, open a Firewall Policy.

   See "Editing a policy" on page 97.

2. In the Firewall Policy page, click **Peer-to-Peer Authentication Settings**.
3. On the Peer-to-Peer Authentication Settings pane, check **Enable peer-to-peer authentication**.
4. Configure each of the values that is listed on the page.

   For more information about these options, click **Help**.

5. To allow remote computers to connect to the client computer without being authenticated, check **Exclude hosts from authentication**, and then click **Excluded Hosts**.

   The client computer allows traffic to the computers listed in the Host List.

6. In the Excluded Hosts dialog box, click **Add** to add the remote computers that do not have to be authenticated.
7. In the Host dialog box, define the host by IP address, IP range, or the subnet, and then click **OK**.
8. In the Excluded Hosts dialog box, click **OK**.
9. When you are done with the configuration of this policy, click **OK**.
10. If you are prompted, assign the policy to a location.

    See "Assigning a shared policy" on page 98.

Chapter 29

Configuring intrusion prevention

This chapter includes the following topics:

About the intrusion prevention system

The intrusion prevention system (IPS) is the Symantec Endpoint Protection client's second layer of defense after the firewall. The IPS is a network-based system that operates on every computer on which the client is installed and the intrusion prevention system is enabled. If a known attack is detected, one or more intrusion prevention technologies can automatically block it.

The intrusion prevention system scans each packet that enters and exits computers in the network for attack signatures. Attack signatures are the packet sequences that identify an attacker's attempt to exploit a known operating system or program vulnerability.

If the information matches a known attack, the IPS automatically discards the packet. The IPS can also sever the connection with the computer that sent the data for a specified amount of time. This feature is called active response, and it protects computers on your network from being affected in any way.

The client includes the following types of IPS engines that identify attack signatures.

Symantec IPS signatures	The Symantec IPS signatures use a stream-based engine that scans multiple packets. Symantec IPS signatures intercept network data at the session layer and capture segments of the messages that are passed back and forth between an application and the network stack. See "About the Symantec IPS signatures" on page 484.
Custom IPS signatures	The custom IPS signatures use a packet-based engine that scans each packet individually. See "About custom IPS signatures" on page 484.

The intrusion prevention system logs the detected attacks in the Security log. You can enable the custom IPS signatures to log detected attacks in the Packet log.

About the Symantec IPS signatures

The Symantec IPS examines packets in two ways. It scans each packet individually by looking for the patterns that do not adhere to specifications and that can crash the TCP/IP stack. It also monitors the packets as a stream of information. It monitors by looking for the commands that are directed at a particular service to exploit or crash the system. The IPS can remember the list of patterns or partial patterns from previous packets and can apply this information to subsequent packet inspections.

The IPS relies on an extensive list of attack signatures to detect and block suspicious network activity. The Symantec Security Response team supplies the known threat list, which you can update on the client by using Symantec LiveUpdate. You download the signatures to the console and then use a LiveUpdate Content Policy to download them to the client. The Symantec IPS engine and the corresponding set of IPS signatures are installed on the client by default.

See "Configuring a LiveUpdate Content Policy" on page 145.

You can also change the behavior of the Symantec IPS signatures.

See "Changing the behavior of Symantec IPS signatures" on page 487.

About custom IPS signatures

The client contains an additional IPS engine that supports packet-based signatures. Both the stream-based and packet-based engines detect signatures in the network data that attack the TCP/IP stack, operating system components, and the application layer. But packet-based signatures can detect attacks in the TCP/IP stack earlier than stream-based signatures.

The packet-based engine does not detect the signatures that span multiple packets. The packet-based IPS engine is more limited in that it does not buffer partial matches and scans single packet payloads only.

Packet-based signatures examine a single packet that matches a rule. The rule is based on various criteria, such as port, protocol, source or destination IP address, TCP flag number, or an application. For example, a custom signature can monitor the packets of information that are received for the string "phf" in GET / cgi-bin/phf? as an indicator of a CGI program attack. Each packet is evaluated for that specific pattern. If the packet of traffic matches the rule, the client allows or blocks the packet and optionally logs the event in the Packet log.

A custom IPS signature includes the following parts:

- Descriptive name
  The name and the description appears in the Security Log and optionally the Packet Log.
- Optional description
- Severity
  Provides a level of severity for the event in the Security Log if the event triggers the signature.
- Traffic direction
- Content
  The content is the syntax. Use the following standard syntax:

  ```
  rule protocol-type, [protocol-options,] [ip-protocol options,]
  msg, content...
  ```

  - rule *protocol-type*, [*protocol-options*,] [*ip-protocol option*,] = The traffic description.
  - msg = The text string that appears in the Security Log.
  - content = The string that is matched against the payload component in the packet for a possible match.
- Optional application
  Optionally, you can provide the application name that triggers the signature. The IPS engine can then match the signature for only the specified applications instead of all applications. By providing the application name, you can also help reduce the false positives that other applications may generate.
- Action to be taken when the event triggers the signature.
  When a signature is triggered, the traffic is allowed or blocked and this action is logged in the Security Log. You should block the traffic if the severity is high. Allow the traffic if you only want to monitor the traffic. You can optionally

write the event to the Packet Log. The Packet Log contains a packet dump of the transaction.

Signatures can cause false positives because they are often based on regular expressions and string matches. The custom signatures use both criteria to look for strings when trying to match a packet.

The client does not include custom signatures by default. You create custom IPS signatures.

See "Creating custom IPS signatures" on page 491.

Configuring intrusion prevention

The default IPS settings protect the client computers against a wide variety of threats. You can customize the default settings for your network. You can customize the IPS settings in one or more of the following ways:

- Enable intrusion prevention settings.
  See "Enabling intrusion prevention settings" on page 487.
- Change the behavior of specific attack signatures.
  See "Changing the behavior of Symantec IPS signatures" on page 487.
- Exclude specific computers from being scanned.
  See "Setting up a list of excluded computers" on page 490.
- Block an attacking computer automatically.
  See " Blocking an attacking computer" on page 489.
- Enable intrusion prevention notifications.
  See "Configuring notifications for Network Threat Protection" on page 511.
- Create custom IPS signatures.
  See "Creating custom IPS signatures" on page 491.

About working with Intrusion Prevention Policies

Except for custom IPS signatures and intrusion prevention notifications, when you configure intrusion prevention, you create an Intrusion Prevention Policy. For custom IPS signatures, you create a custom IPS library.

You create and edit Intrusion Prevention Policies similar to the way you create and modify other types of policies. You can assign, withdraw, replace, copy, export, import, or delete an Intrusion Prevention Policy or Custom Intrusion Prevention Library.

You typically assign a policy to multiple groups in your security network. You can create a non-shared, location-specific policy if you have specific requirements for a particular location.

The procedures in this chapter assume that you are familiar with the basics of policy configuration.

See "Using policies to manage your network security" on page 90.

Enabling intrusion prevention settings

You can block certain types of attacks on the client, depending on the intrusion prevention technology that you select.

You must enable the intrusion prevention settings to enable either the Symantec IPS signature engine or the custom IPS signature engine. If you do not enable this setting, the client ignores possible attack signatures.

Note: To configure these settings in mixed control, you must also enable these settings in the Client User Interface Mixed Control Settings dialog box.

See "Configuring Network Threat Protection settings for mixed control" on page 499.

For more information about these options, click **Help**.

To enable intrusion prevention settings

1. In the console, open an Intrusion Prevention Policy.

   See "Editing a policy" on page 97.

2. On the Intrusion Prevention Policy page, click **Settings**.
3. On the Settings page, check the following check boxes that apply:
   - **Enable Intrusion Prevention**
   - **Enable denial of service detection**
   - **Enable port scan detection**
4. When you finish configuring this policy, click **OK**.

   See "Setting up a list of excluded computers" on page 490.

Changing the behavior of Symantec IPS signatures

You may want to change the default behavior of the Symantec IPS signatures for the following reasons:

- To reduce the possibility of a false positive. In some cases, benign network activity may appear similar to an attack signature. If you receive repeated warnings about possible attacks, and you know that these attacks are being triggered by safe behavior, you can exclude the attack signature that matches the benign activity.
- To reduce resource consumption by reducing the number of attack signatures for which the client checks. However, you must be certain that an attack signature poses no threat before excluding it from blocking.

You can change the action that the client takes when the IPS recognizes an attack signature. You can also change whether the client logs the event in the Security log.

Note: To change the behavior of a custom IPS signature that you create or import, you edit the signature directly.

To change the behavior of Symantec IPS signatures

1. In the console, open an Intrusion Prevention Policy.

   See "Editing a policy" on page 97.

2. On the Intrusion Prevention Policy page, click **Exceptions**.
3. On the Exceptions page, click **Add**.
4. In the Add Intrusion Prevention Exceptions dialog box, do one of the following actions to filter the signatures:
   - To display the signatures in a particular category, select an option from the Show category drop-down list.
   - To display the signatures that are classified with a particular severity, select an option from the Show severity drop-down list.
5. Select one or more IPS signatures.

   To make the behavior for all signatures the same, click **Select All**.
6. Click **Next**.
7. In the Signature Action dialog box, change the action from Block to Allow or from Allow to Block.
8. Optionally, change the log action in either one of the following ways:
   - Change **Log the traffic** to **Do not log the traffic**.
   - Change **Do not log the traffic** to **Log the traffic**.

9 Click **OK**.

If you want to remove the exception and revert the signature's behavior back to the original behavior, select the signature and click **Delete**.

10 Click **OK**.

11 If you want to change the behavior of other signatures, repeat steps 3 to 10.

12 When you finish configuring this policy, click **OK**.

To remove the exception

1 In the console, open an Intrusion Prevention Policy.

See "Editing a policy" on page 97.

2 On the Intrusion Prevention Policy page, click **Exceptions**.

3 On the Exceptions pane, select the exception you want to remove and click **Delete**.

4 When you are asked to confirm the deletion, click **Yes**.

Blocking an attacking computer

If the Symantec Endpoint Protection client detects a network attack, it can automatically block the connection to ensure that the client computer is safe. The client activates an active response, which automatically blocks all communication to and from the attacking computer for a set period of time. The IP address of the attacking computer is blocked for a single location.

The attacker's IP address is recorded in the Security log. In client control, users can unblock an attack by stopping the active response in the Security log.

If you set the client to mixed control, you can specify whether the setting is available or not available on the client for the user to enable. If not available, you must enable it in the Client User Interface Mixed Control Settings dialog box.

See "Configuring Network Threat Protection settings for mixed control" on page 499.

Updated IPS signatures, updated denial-of-service signatures, port scans, and MAC spoofing also trigger an active response.

To block an attacking computer

1 In the console, open an Intrusion Prevention Policy.

See "Editing a policy" on page 97.

2 On the Intrusion Prevention Policy page, click **Settings**.

3 On the Settings page, check **Automatically block an attacker's IP address**.

4 In the **Number of seconds during which to block IP address ... seconds** text box, specify the number of seconds to block potential attackers.

Enter a number from one second to 999,999 seconds.

5 When you finish configuring this policy, click **OK**.

Setting up a list of excluded computers

The Symantec Endpoint Protection client may define some normal Internet activities as attacks. For example, some Internet service providers scan the ports of the computer to ensure that you are within their service agreements. Or, you may have some computers in your internal network that you want to set up for testing purposes.

You can set up a list of computers for which the client does not match attack signatures or check for port scans or denial-of-service attacks. The client allows all inbound traffic and outbound traffic from these hosts, regardless of the firewall rules and settings or IPS signatures.

Note: You can also set up a list of computers that allows all inbound traffic and outbound traffic unless an IPS signature detects an attack. In this case, you create a firewall rule that allows all hosts.

To set up a list of excluded computers

1 In the console, open an Intrusion Prevention Policy.

See "Editing a policy" on page 97.

2 On the Intrusion Prevention Policy page, click **Settings**.

3 If not checked already, check **Enable excluded hosts** and then click **Excluded Hosts**.

4 In the Excluded Hosts dialog box, click **Add**.

5 In the Host dialog box, in the drop-down list, select one of the following host types:

- IP address
- IP range
- Subnet

6 Enter the appropriate information that is associated with the host type you selected.

For more information about these options, click **Help**.

7 Click **OK**.

8 Repeat 4 and 7 to add additional devices and computers to the list of excluded computers.

9 To edit or delete any of the excluded hosts, select a row, and then click **Edit** or **Delete**.

10 Click **OK**.

11 When you finish configuring the policy, click **OK**.

Creating custom IPS signatures

You can write your own signatures to identify a specific intrusion and reduce the possibility of signatures that cause a false positive. The more information you can add to a custom signature, the more effective the signature is.

When you create a custom library, you can organize signatures into signature groups to manage them more easily. You must add at least one signature group to a custom signature library before you add the signatures to the signature group. You can copy and paste signatures between groups and between libraries.

Warning: You must be familiar with the TCP, UDP, or ICMP protocols before you develop intrusion prevention signatures. An incorrectly formed signature can corrupt the custom IPS library and damage the integrity of the clients.

To create custom IPS signatures, you must complete the following steps:

- Create a custom IPS library.
- Add a signature.

To create a custom IPS library

1 In the console, click **Policies**, and then click **Intrusion Prevention**.

2 Under Tasks, click **Add Custom Intrusion Prevention Signatures**.

3 In the Custom Intrusion Prevention Signatures dialog box, type a name and optional description for the library.

The NetBIOS Group is a sample signature group with one sample signature. You can edit the existing group or add a new group.

4 To add a new group, on the Signatures tab, under the Signature Groups list, click **Add**.

5 In the Intrusion Prevention Signature Group dialog box, type a group name and optional description, and then click **OK**.

The group is enabled by default. If the signature group is enabled, all signatures within the group are enabled automatically. To retain the group for reference but to disable it, uncheck **Enable this group**.

6 Add a custom signature.

To add a custom signature

1 Create a custom IPS library.

2 On the Signatures tab, under Signatures for this Group, click **Add**.

3 In the Add Signature dialog box, type a name and optional description for the signature.

4 In the Severity drop-down list, select a severity level.

Events that match the signature conditions are logged with this severity.

5 In the Direction drop-down list, specify the traffic direction that you want the signature to check.

6 In the Content field, type the syntax of the signature.

For more information on the syntax, click **Help**.

7 If you want an application to trigger the signature, click **Add**.

8 In the Add Application dialog box, type the file name and an optional description for the application.

For example, to add the application Internet Explorer, type the file name as **iexplore** or **iexplore.exe**. If you do not specify a file name, any application can trigger the signature.

9 Click **OK**.

The added application is enabled by default. If you want to disable the application until a later time, uncheck the check box in the Enabled column.

10 In the Action group box, select the action you want the client to take when the signature detects the event:

Block	Identifies and blocks the event or attack and records it in the Security Log
Allow	Identifies and allows the event or attack and records it in the Security Log

11 To record the event or attack in the Packet Log, check **Write to Packet Log**.

12 Click **OK**.

The added signature is enabled by default. If you want to disable the signature until a later time, uncheck the check box in the Enabled column.

13 To add additional signatures to the signature group, repeat steps 2 to 12.

To edit or delete a signature, select it and then click **Edit** or **Delete**.

14 If you are finished with the configuration of this library, click **OK**.

15 If you are prompted, assign the custom IPS signatures to a group.

See "Assigning a shared policy" on page 98.

You can also assign multiple custom IPS libraries to a group.

See "Assigning multiple custom IPS libraries to a group" on page 493.

Assigning multiple custom IPS libraries to a group

After you create a custom IPS library, you assign it to a group rather than an individual location. You can later assign additional custom IPS libraries to the group.

To assign multiple custom IPS libraries to a group

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

2 Under View Clients, select the group to which you want to assign the custom signatures.

3 On the Policies tab, under Location-independent Policies and Settings, click **Custom Intrusion Prevention**.

4 In the Custom Intrusion Prevention for *group name* dialog box, check the check box in the Enabled column for each custom IPS library you want to assign to that group.

5 Click **OK**.

Changing the order of signatures

The IPS engine for custom signatures checks the signatures in the order that they are listed in the signatures list. Only one signature is triggered per packet. When a signature matches an inbound traffic packet or outbound traffic packet, the IPS engine stops checking other signatures. So that the IPS engine executes signatures in the correct order, you can change the order of the signatures in the signatures list. If multiple signatures match, move the higher priority signatures to the top.

For example, if you add a signature group to block TCP traffic in both directions on destination port 80, you might add the following signatures:

- Block all traffic on port 80
- Allow all traffic on port 80

If the Block all traffic signature is listed first, the Allow all traffic signature is never enacted. If the Allow all traffic signature is listed first, the Block all traffic signature is never enacted, and all HTTP traffic is always allowed.

To change the order of signatures

1. Open a custom IPS library.
2. Add or edit a signature.

   See "To add a custom signature" on page 492.
3. On the Signatures tab, in the Signatures for this Group table, select the signature that you want to move, and then do one of the following actions:
   - To process this signature before the signature above it, click **Move Up**.
   - To process this signature after the signature below it, click **Move Down**.
4. When you finish configuring this library, click **OK**.

Copying and pasting signatures

You can copy and paste signatures within the same signature group, between signature groups, or between signature libraries. For example, you may realize that you added a signature to the wrong signature group. Or you may want to have two signatures that are nearly identical.

To copy and paste signatures

1. Open a custom IPS library.
2. In the Custom Intrusion Prevention Signatures dialog box, in the Signatures tab, in the Signatures for this Group table, right-click the signature you want to copy, and then click **Copy**.
3. Right-click the signatures list, and then click **Paste**.
4. When you finish configuring this library, click **OK**.

Defining variables for signatures

When you add a custom IPS signature, you can use variables to represent changeable data in signatures. If the data changes, you can edit the variable instead of editing the signatures throughout the library.

Before you can use the variables in the signature, you must define them. The variables you define in the custom signature library can then be used in any signature in that library.

You can copy and paste the content from the existing sample variable to start as a basis for creating content.

To define variables

1. Create a custom IPS library.
2. In the Custom Intrusion Prevention Signatures dialog box, click the **Variables** tab.
3. Click **Add**.
4. In the Add Variable dialog box, type a name and optional description for the variable.
5. Add a content string for the variable value of up to 255 characters.

   When you enter the variable content string, follow the same syntax guidelines that you use for entering values into signature content.
6. Click **OK**.

   After the variable is added to the table, you can use the variable in any signature in the custom library.

To use variables in signatures

1. On the Signatures tab, add or edit a signature.

   See "To add a custom signature" on page 492.
2. In the Add Signature or Edit Signature dialog box, in the Content field, type the variable name with a dollar sign ($) in front of it.

   For example, if you create a variable named HTTP for specifying HTTP ports, type the following:

   $HTTP
3. Click **OK**.
4. When you finish configuring this library, click **OK**.

Chapter 30

Customizing Network Threat Protection

This chapter includes the following topics:

Enabling and disabling Network Threat Protection

By default, Network Threat Protection is enabled. You may want to disable Network Threat Protection on selected computers. For example, you might need to install a patch on the client computers that would otherwise force the firewall to block the installation.

If you disable Network Threat Protection, it is automatically enabled when the following happens:

- The user shuts down and restarts the client computer.
- The client location changes from server control to client control.
- You configured the client to enable protection after a certain period of time.
- A new security policy that enable protection is downloaded to the client.

You can also manually enable Network Threat Protection from the computer status logs.

See "Running commands and actions from logs" on page 274.

You can also give the user on the client computer permission to enable or disable protection. However, you can override the client's setting. Or you can disable protection on the client even if users have enabled it. You can enable protection even if users have disabled it.

See "Configuring user interface settings" on page 168.

To enable and disable Network Threat Protection for a group

1. In the console, click **Clients**.
2. Under View Clients, select a group for which you want to enable or disable protection.
3. Do one of the following actions:
   - For all computers and users in group, right-click the group, click **Run Command on Group**, and then click **Enable Network Threat Protection** or **Disable Network Threat Protection**.
   - For selected users or computers within a group, on the Clients tab, select the users or computers. Then right-click the selection and click **Run Command on Clients > Enable Network Threat Protection** or **Disable Network Threat Protection**.
4. To confirm the action, click **Yes**.
5. Click **OK**.

Configuring Network Threat Protection settings for mixed control

You can set up the client so that users have no control, full control, or limited control over which Network Threat Protection settings they can configure. When you configure the client, use the following guidelines:

- If you set the client to server control, the user cannot create any firewall rules or enable firewall settings and intrusion prevention settings.
- If you set the client to client control, the user can create firewall rules and enable all firewall settings and intrusion prevention settings.
- If you set the client to mixed control, the user can create firewall rules and you decide which firewall settings and intrusion prevention settings the user can enable.

See "Configuring user interface settings" on page 168.

To configure Network Threat Protection settings for mixed control

1. In the console, click **Clients**.
2. Under View Clients, select the group with the user control level you want to modify.
3. On the Policies tab, under Location-specific Policies and Settings, under a location, expand **Location-specific Settings**.
4. To the right of Client User Interface Control Settings, click **Tasks > Edit Settings**.
5. In the Control Mode Settings dialog box, click **Mixed control**, and then click **Customize**.
6. On the Client/Server Control Settings tab, under the Firewall Policy category and Intrusion Prevention Policy category, do one of the following actions:
   - To make a client setting available for the users to configure, click **Client**.
   - To configure a client setting, click **Server**.
7. Click **OK**.

8 Click **OK**.

9 For each firewall setting and intrusion prevention setting that you set to Server, enable or disable the setting in the Firewall Policy or Intrusion Prevention Policy.

See "Enabling Smart traffic filtering" on page 479.

See "Enabling traffic and stealth settings" on page 480.

See "Configuring intrusion prevention" on page 486.

Adding hosts and host groups

A host group is a collection of DNS domain names, DNS host names, IP addresses, IP ranges, MAC addresses, or subnets that are grouped under one name. The purpose of host groups is to eliminate the retyping of host addresses and names. For example, you can add multiple IP addresses one at a time to a firewall rule. Or, you can add multiple IP addresses to a host group, and then add the group to the firewall rule.

As you incorporate host groups, you must describe where the groups are used. If you decide later to delete a host group, you must first remove the host group from all the rules that reference the group.

When you add a host group, it appears at the bottom of the Hosts List. You can access the Hosts list from the Host field in a firewall rule.

See "About host triggers" on page 465.

See "Editing and deleting host groups" on page 501.

To create host groups

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

2 Expand Policy Components, and then click **Host Groups**.

3 Under Tasks, click **Add a Host Group**.

4 In the Host Group dialog box, type a name, and then click **Add**.

5 In the Host dialog box, in the Type drop-down list, select one of the following hosts:

- DNS domain
- DNS host
- IP address
- IP range

- MAC address
- Subnet

6 Enter the appropriate information for each host type.

7 Click **OK**.

8 Add additional hosts, if necessary.

9 Click **OK**.

Editing and deleting host groups

You can edit or delete any custom host groups that you have added. You cannot edit or delete a default host group. Before you can delete a custom host group, you must remove the host group from all the rules that reference the group. The settings that you edit change in all rules that reference the group.

See "Adding hosts and host groups" on page 500.

To edit host groups

1 In the console, click **Policies > Policy Components > Host Groups**.

2 In the Host Groups pane, select the host group you want to edit.

3 Under Tasks, click **Edit the Host Group**.

4 In the Host Group dialog box, optionally edit the group name, select a host, and then click **Edit**.

To remove the host from the group, click **Delete**, and then click **Yes**.

5 In the Host dialog box, change the host type or edit the host settings.

6 Click **OK**.

7 Click **OK**.

To delete host groups

1 In the console, click **Policies > Policy Components > Host Groups**.

2 In the Host Groups pane, select the host group you want to delete.

3 Under Tasks, click **Delete the Host Group**.

4 When you are asked to confirm, click **Delete**.

Adding hosts and host groups to a rule

To block traffic to or from a specific server, block the traffic by IP address rather than by domain name or host name. Otherwise, the user may be able to access the IP address equivalent of the host name.

To add hosts and host groups to a rule

1. In the console, open a Firewall Policy.

   See "Editing a policy" on page 97.

2. On the Firewall Policy page, click **Rules**.
3. On the Rules tab, in the Rules list, select the rule you want to edit, right-click the **Host** field, and then click **Edit**.
4. In the Host List dialog box, do one of the following actions:
   - Click **Source/Destination**.
   - Click **Local/Remote**.
5. In the Source and Destination or Local and Remote tables, do one of the following tasks:
   - To enable a host group that you added through the Policy Components list, go to step 10.
     See "Adding hosts and host groups" on page 500.
   - To add a host for the selected rule only, click **Add**.
6. In the Host dialog box, select a host type from the Type drop-down list, and enter the appropriate information for each host type.

   For more details on each option in this dialog box, click **Help**.
7. Click **OK**.
8. Add additional hosts, if necessary.
9. In the Host List dialog box, for each host or host group that you want to trigger the firewall rule, make sure the check box in the Enabled column is checked.
10. Click **OK** to return to the Rules list.

Adding network services

Network services let networked computers send and receive messages, share files, and print. A network service uses one or more protocols or ports to pass through a specific type of traffic. For example, the HTTP service uses ports 80 and 443 in

the TCP protocol. You can create a firewall rule that allows or blocks network services.

The network service list eliminates the necessity to retype a protocol and port for each rule that you create. You can select a network service from a default list of commonly used network services. You can then add the network service to the firewall rule. You can also add network services to the default list.

See "Adding network services to a rule" on page 504.

Note: IPv4 and IPv6 are the two network layer protocols that are used on the Internet. The firewall blocks attacks that travel through IPv4, but not through IPv6. If you install the client on the computers that run Microsoft Vista, the Rules list includes several default rules that block the Ethernet protocol type of IPv6. If you remove the default rules, you must create a rule that blocks IPv6.

If you want to allow or block a network service that is not in the default list, you can add it. You need to be familiar with the type of protocol and the ports that it uses.

To add a custom network service that is accessible from any firewall rule, you add it through the Policy Components list.

To add a custom network service to the default list

1. In the console, click **Policies**.
2. Expand Policy Components, and then click **Network Services**.
3. Under Tasks, click **Add a Network Service**.
4. In the Network Service dialog box, type a name for the service, and then click **Add**.
5. From the Protocol drop-down list, select one of the following protocols:
   - TCP
   - UDP
   - ICMP
   - IP
   - Ethernet

   The options change, based on which protocol you select. For more information, click **Help**.
6. Fill in the appropriate fields, and then click **OK**.

7 Add one or more additional protocols, as necessary.

8 Click **OK**.

You can add the service to any firewall rule.

Editing and deleting custom network services

You can edit or delete any custom network services that you have added. You cannot edit or delete a default network service. Before you can delete a custom network service, you must remove it from all the rules that reference the service.

See "Adding network services" on page 502.

To edit custom network services

1 In the console, click **Policies > Policy Components > Network Services**.

2 In the Network Services pane, select the service that you want to edit.

3 Under Tasks, click **Edit the Network Service**.

4 In the Network Service dialog box, change the service name, or select the protocol and click **Edit**.

5 Change the protocol settings.

For information about the options in this dialog box, click **Help**.

6 Click **OK**.

7 Click **OK**.

To delete custom network services

1 In the console, click **Policies > Policy Components > Network Services**.

2 In the Network Service pane, select the service that you want to delete.

3 Under Tasks, click **Delete the Network Service**.

4 When you are asked to confirm, click **Yes**.

Adding network services to a rule

You can add a custom network service through a firewall rule. However, that network service is not added to the default list. You cannot access the custom adapter from any other rule.

See "Adding network services" on page 502.

To add network services to a rule

1 In the console, open a Firewall Policy.

See "Editing a policy" on page 97.

2 On the Firewall Policy page, click **Rules**.

3 On the Rules tab, in the Rules list, select the rule you want to edit, right-click the Service field, and then click **Edit**.

4 In the Service List dialog box, check the **Enable** check box for each service that you want to trigger the rule.

5 To add an additional service for the selected rule only, click **Add**.

6 In the Protocol dialog box, select a protocol from the Protocol drop-down list.

7 Fill out the appropriate fields.

For more information on these options, click **Help**.

8 Click **OK**.

9 Click **OK**.

10 Click **OK**.

Enabling network file and printer sharing

You can enable the client to either share its files or to browse for shared files and printers on the local network. To prevent network-based attacks, you may want to disable network file and printer sharing.

You enable network file and print sharing by adding firewall rules. The firewall rules allow access to the ports to browse and share files and printers. You create one firewall rule so that the client can share its files. You create a second firewall rule so that the client can browse for other files and printers.

If the client is in client control or mixed control, users on the client can enable these settings automatically by configuring them in Network Threat Protection. In mixed control, a server firewall rule that specifies this type of traffic can override these settings. In server control, these settings are not available on the client.

To enable clients to browse for files and printers

1 In the console, open a Firewall Policy.

See "Editing a policy" on page 97.

2 On the Firewall Policy page, click **Rules**.

3 Add a blank rule, and in the Name column, type a name for the rule.

See “Adding blank rules” on page 473.

4 Right-click the Service field, and then click **Edit**.

5 In the Service List dialog box, click **Add**.

6 In the Protocol dialog box, in the Protocol drop-down list, click **TCP**, and then click **Local/Remote**.

7 In the Remote port drop-down list, type **88, 135, 139, 445**

8 Click **OK**.

9 In the Service List dialog box, click **Add**.

10 In the Protocol dialog box, in the Protocol drop-down list, click **UDP**.

11 In the Local Port drop-down list, type **137, 138**

12 In the Remote Port drop-down list, type **88**

13 Click **OK**.

14 In the Service List dialog box, make sure the two services are enabled, and then click **OK**.

15 On the Rules tab, make sure the Action field is set to **Allow**.

16 If you are done with the configuration of the policy, click **OK**.

17 If you are prompted, assign the policy to a location.

See “Assigning a shared policy” on page 98.

To enable other computers to browse files on the client

1 In the console, open a Firewall Policy.

See “Editing a policy” on page 97.

2 On the Firewall Policy page, click **Rules**.

3 Add a blank rule, and in the Name column, type a name for the rule.

See “Adding blank rules” on page 473.

4 Right-click the Service field, and then click **Edit**.

5 In the Service List dialog box, click **Add**.

6 In the Protocol dialog box, in the Protocol drop-down list, click **TCP**, and then click **Local/Remote**.

7 In the Local Port drop-down list, type **88, 135, 139, 445**

8 Click **OK**.

9 In the Service List dialog box, click **Add**.

10 In the Protocol dialog box, in the Protocol drop-down list, click **UDP**.

11 In the Local Port drop-down list, type **88, 137, 138**

12 Click **OK**.

13 In the Service List dialog box, make sure the two services are enabled, and then click **OK**.

14 On the Rules tab, make sure the Action field is set to **Allow**.

15 If you are done with the configuration of the policy, click **OK**.

16 If you are prompted, assign the policy to a location.

See "Assigning a shared policy" on page 98.

Adding network adapters

You can apply a separate firewall rule to each network adapter. For example, you may want to block traffic through a VPN at an office location, but not at a home location.

You can select a network adapter from a default list that is shared across Firewall Policies and rules. The most common adapters are included in the default list in the Policy Components list. The common adapters include VPNs, Ethernet, wireless, Cisco, Nortel, and Enterasys adapters. Use the default list so that you do not have to retype each network adapter for every rule you create.

Note: The client does not filter or detect network traffic from PDA (personal digital assistant) devices.

See "Adding network adapters to a rule" on page 508.

See "Editing and deleting custom network adapters" on page 509.

To add a custom network adapter to the default list

1 In the console, click **Policies > Policy Components > Network Adapters**.

2 Under Tasks, click **Add a Network Adapter**.

3 In the Network Adapter dialog box, in the Adapter Type drop-down list, select an adapter.

4 In the Adapter Name field, optionally type a description.

5 In the Adapter Identification text box, type the case-sensitive brand name of the adapter.

To find the brand name of the adapter, open a command line on the client, and then type the following text:

```
ipconfig/all
```

6 Click **OK**.

You can then add the adapter to any firewall rule.

Adding network adapters to a rule

You can add a custom network adapter from a firewall rule. However, that adapter is not added to the shared list. You cannot access the custom adapter from any other rule.

See "Adding network adapters" on page 507.

To add a network adapter to a rule

1 In the console, open a Firewall Policy.

See "Editing a policy" on page 97.

2 On the Firewall Policy page, click **Rules**.

3 On the Rules tab, in the Rules list, select the rule you want to edit, right-click the **Adapter** field, and then click **More Adapters**.

4 In the Network Adapter dialog box, do one of the following actions:

- To trigger the rule for any adapter, even if it is not listed, click **Apply the rule to all adapters**, and then go to step 8.
- To trigger the rule for selected adapters, click **Apply the rule to the following adapters**, and then check the check box in the Enabled column for each adapter that you want to trigger the rule.

5 To add a custom adapter for the selected rule only, click **Add**.

6 In the Network Adapter dialog box, select the adapter type and type the adapter's brand name in the Adapter Identification text field.

7 Click **OK**.

8 Click **OK**.

9 Click **OK**.

Editing and deleting custom network adapters

You can edit or delete any custom network adapters that you have added. You cannot edit or delete a default network adapter. Before you can delete a custom adapter, you must remove it from all the rules that reference the adapter. The settings that you edit change in all rules that reference the adapter.

See "Adding network adapters" on page 507.

To edit a custom network adapter

1. In the console, click **Policies**.
2. Under Policy Components, click **Network Adapters**.
3. In the Network Adapters pane, select the custom adapter you want to edit.
4. Under Tasks, click **Edit the Network Adapter**.
5. In the Network Adapter dialog box, edit the adapter type, name, or adapter identification text.
6. Click **OK**.

To delete a custom network adapter

1. In the console, click **Policies**.
2. Under Policy Components, click **Network Adapters**.
3. In the Network Adapters pane, select the custom adapter you want to delete.
4. Under Tasks, click **Delete the Network Adapter**.
5. When you are asked to confirm, click **Yes**.

Adding applications to a rule

You can define information about the applications that clients run and include this information in a firewall rule. For example, you might want to allow old versions of Microsoft Word.

You can define applications in the following ways:

- You can define the characteristics of an application by entering the information manually. If you do not have enough information, you may want to search the learned applications list.
- You can define the characteristics of an application by searching the learned applications list. Applications in the learned applications list are the applications that client computers in your network run.

To define applications

1. In the console, open a Firewall Policy.

   See "Editing a policy" on page 97.

2. On the Firewall Policies page, click **Rules**.
3. On the Rules tab, in the Rules list, right-click the **Application** field, and then click **Edit**.
4. In the Application List dialog box, click **Add**.
5. In the Add Application dialog box, enter one or more of the following fields:
   - Path and file name
   - Description
   - Size, in bytes
   - Date that the application was last changed
   - File fingerprint
6. Click **OK**.
7. Click **OK**.

To search for applications from the learned applications list

1. On the Firewall Policies page, click **Rules**.
2. On the Rules tab, select a rule, right-click the **Application** field, and then click **Edit**.
3. In the Application List dialog box, click **Add From**.
4. In the Search for Applications dialog box, search for an application.

   See "Searching for information about the applications that the computers run" on page 115.

5. Under the Query Results table, to add the application to the Applications list, select the application, click **Add**, and then click **OK**.
6. Click **Close**.
7. Click **OK**.

Adding schedules to a rule

You can set up a time period when a rule is active or not active.

To add schedules to a rule

1. In the console, open a Firewall Policy.

   See "Editing a policy" on page 97.

2. On the Firewall Policy page, click **Rules**.
3. On the Rules tab, select the rule you want to edit, right-click the **Time** field, and then click **Edit**.
4. In the Schedule List dialog box, click **Add**.
5. In the Add Schedule dialog box, configure the start time and end time that you want the rule to be active or not active.
6. In the Month drop-down list, select either **All** or a specific month.
7. Check one of the following check boxes:
   - Every day
   - Weekends
   - Weekdays
   - Specify days
     If you check Specify days, check one or more of the listed days.
8. Click **OK**.
9. In the Schedule List, do one of the following actions:
   - To keep the rule active during this time, uncheck the check box in the Any Time Except column.
   - To make the rule inactive during this time, check the check box in the Any Time Except column.
10. Click **OK**.

Configuring notifications for Network Threat Protection

By default, notifications appear on client computers when the client detects various Network Threat Protection events. You can enable some of these notifications. Enabled notifications display a standard message. You can add customized text to the standard message.

Table 30-1 displays the types of events that you can enable and configure.

Table 30-1 Network Threat Protection notifications

Notification type	Notification type	Description
Display notification on the computer when the client blocks an application	Firewall	A firewall rule on the client blocks an application. You can enable or disable this notification and add additional text to the notification.
Additional text to display if the action for a firewall rule is 'Ask'	Firewall	The applications on the client try to access the network. This notification is always enabled and can't be disabled.
Display Intrusion Prevention notifications	Intrusion prevention	The client detects an intrusion prevention attack. You can enable or disable this notification in server control or mixed control.

To configure firewall notifications

1. In the console, open a Firewall Policy.

   See "Editing a policy" on page 97.

2. On the **Firewall Policy** page, click **Rules**.
3. On the **Notifications** tab, check **Display notification on the computer when the client blocks an application**.
4. To add customized text to the standard message that appears when a rule's action is set to Ask, check **Additional text to display if the action for a firewall rule is 'Ask'**.
5. For either notification, click **Set Additional Text**.
6. In the **Enter Additional Text** dialog box, type the additional text you want the notification to display, and then click **OK**.
7. When you are done with the configuration of this policy, click **OK**.

To configure intrusion prevention notifications

1. In the console, click **Clients** and under **View Clients**, select a group.
2. On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.
3. To the right of **Client User Interface Control Settings**, click **Tasks** , and then click **Edit Settings**.
4. In the **Client User Interface Control Settings for *group name*** dialog box, click either **Server control** or **Mixed control**.

5 Beside **Mixed control** or **Server control**, click **Customize**.

If you click **Mixed control**, on the **Client/Server Control Settings tab**, beside **Show/Hide Intrusion Prevention notifications**, click **Server**. Then click the **Client User Interface Settings** tab.

6 In the **Client User Interface Settings** dialog box or tab, click **Display Intrusion Prevention notifications**.

7 To enable a beep when the notification appears, click **Use sound when notifying users**.

8 In the **Number of seconds to display notifications** text field, type the number of seconds that you want the notification to appear.

9 To add text to the standard notification that appears, click **Additional Text**.

10 In the **Additional Text** dialog box, type the additional text you want the notification to display, and then click **OK**.

11 Click **OK**.

12 Click **OK**.

Configuring email messages for traffic events

You can configure the Symantec Endpoint Protection Manager to send an email message to you each time the firewall detects a rule violation, attack, or event. For example, you may want to know when a client blocks the traffic that comes from a particular IP address.

To configure email messages for traffic events

1 In the console, open a Firewall Policy.

See "Editing a policy" on page 97.

2 On the **Firewall Policy** page, click **Rules**.

3 On the **Rules** tab, select a rule, right-click the **Logging** field, and do the following actions:

- To send an email message when a firewall rule is triggered, check **Send Email Alert**.
- To generate a log event when a firewall rule is triggered, check both **Write to Traffic Log** and **Write to Packet Log**.

4 When you are done with the configuration of this policy, click **OK**.

5 Configure a security alert.

See "Creating administrator notifications" on page 283.

6 Configure a mail server.

See "Establishing communication between Symantec Endpoint Protection Manager and email servers" on page 327.

Setting up network application monitoring

You can configure the client to detect and monitor any application that runs on the client computer and that is networked. Network applications send and receive traffic. The client detects whether an application's content changes.

An application's content changes for the following reasons:

- A Trojan horse attacked the application.
- The application was updated with a new version or an update.

If you suspect that a Trojan horse has attacked an application, you can use network application monitoring to configure the client to block the application. You can also configure the client to ask users whether to allow or block the application.

Network application monitoring tracks an application's behavior in the Security Log. If an application's content is modified too frequently, it is likely that a Trojan horse attacked the application and the client computer is not safe. If an application's content is modified on an infrequent basis, it is likely that a patch was installed and the client computer is safe. You can use this information to create a firewall rule that allows or blocks an application.

You can add applications to a list so that the client does not monitor them. You may want to exclude the applications that you think are safe from a Trojan horse attack, but that have frequent and automatic patch updates.

You may want to disable network application monitoring if you are confident that the client computers receive adequate protection from Antivirus and Antispyware Protection. You may also want to minimize the number of notifications that ask users to allow or block a network application.

To set up network application monitoring

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

2 Under View Clients, select a group, and then click **Policies**.

3 On the Policies tab, under Location-independent Policies and Settings, click **Network Application Monitoring**.

4 In the Network Application Monitoring for *group name* dialog box, click **Enable Network Application Monitoring**.

5 In the **When an application change is detected** drop-down list, select the action that the firewall takes on the application that runs on the client:

- Ask
  Asks the user to allow or block the application.
- Block the traffic
  Blocks the application from running.
- Allow and Log
  Allows the application to run and records the information in the Security Log.
  The firewall takes this action on the applications that have been modified only.

6 If you selected Ask, click **Additional Text**.

7 In the Additional Text dialog box, type the text that you want to appear under the standard message, and then click **OK**.

8 To exclude an application from being monitored, under Unmonitored Application List, do one of the following actions:

- To define an application manually, click **Add**, fill out one or more fields, and then click **OK**.
- To define an application from a learned applications list, click **Add From**.
  See "Searching for information about the applications that the computers run" on page 115.
  The learned applications feature must be enabled.
  See "Configuring the management server to collect information about the applications that the client computers run" on page 113.

The learned applications list monitors both networked and non-networked applications. You must select networked applications only from the learned applications list. After you have added applications to the Unmonitored Applications List, you can enable, disable, edit, or delete them.

9 To enable or disable an application, check the check box in the Enabled column.

10 Click **OK**.

Section 5

Configuring Proactive Threat Protection

Chapter 31

Configuring TruScan proactive threat scans

This chapter includes the following topics:

About TruScan proactive threat scans

TruScan proactive threat scans provide an additional level of protection to your computer. Proactive threat scans complement your existing antivirus, antispyware, intrusion prevention, and firewall protection technologies.

Antivirus and antispyware scans rely mostly on signatures to detect known threats. Proactive threat scans use heuristics to detect unknown threats. Heuristic process scans analyze the behavior of an application or a process. The scan determines if the process exhibits characteristics of threats, such as Trojan horses, worms,

or keyloggers. This type of protection is sometimes referred to as protection from zero-day attacks.

See "About the processes that TruScan proactive threat scans detect" on page 521.

Note: Auto-Protect also uses a type of heuristic called Bloodhound to detect suspicious behavior in files. Proactive threat scans detect suspicious behavior in active processes.

You include settings about proactive threat scans as part of an Antivirus and Antispyware Policy. Many of the settings can be locked so that users on client computers cannot change the settings.

You can configure the following settings:

- What types of threats to scan for
- How often to run proactive threat scans
- Whether or not notifications should appear on the client computer when a proactive threat detection occurs

TruScan proactive threat scans are enabled when both the Scan for Trojan horses and worms or Scan for keyloggers settings are enabled. If either setting is disabled, the Status page in the Symantec Endpoint Protection client shows Proactive Threat Protection as disabled.

Proactive threat scanning is enabled by default.

Note: Since proactive threat scans analyze applications and processes for behavior anomalies, they can impact your computer's performance.

About using the Symantec default settings

You can decide how you want to manage proactive threat detections. You can use the Symantec defaults, or you can specify the sensitivity level and the detection action.

If you choose to allow Symantec to manage the detections, the client software determines the action and the sensitivity level. The scan engine that runs on the client computer determines the default setting. If you choose to manage the detections instead, you can set a single detection action and a specific sensitivity level.

To minimize false positive detections, Symantec recommends that you use the Symantec-managed defaults initially. After a certain length of time, you can

observe the number of false positives that the clients detect. If the number is low, you might want to tune the proactive threat scan settings gradually. For example, for detection of Trojan horses and worms, you might want to move the sensitivity slider slightly higher than its default. You can observe the results of the proactive threat scans that run after you set the new configuration.

See "Understanding TruScan proactive threat detections" on page 528.

See "Specifying the actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers" on page 530.

About the processes that TruScan proactive threat scans detect

Proactive threat scans detect the processes that behave similarly to Trojan horses, worms, or keyloggers. The processes typically exhibit a type of behavior that a threat can exploit, such as opening a port on a user's computer.

You can configure settings for some types of proactive threat detections. You can enable or disable the detection of processes that behave like Trojan horses, worms, or keyloggers. For example, you might want to detect the processes that behave like Trojan horses and worms, but not processes that behave like keylogger applications.

Symantec maintains a list of commercial applications that could be used for malicious purposes. The list includes the commercial applications that record user keystrokes. It also includes the applications that control a client computer remotely. You might want to know if these types of applications are installed on client computers. By default, proactive threat scans detect these applications and log the event. You can specify different remediation actions.

You can configure the type of remediation action that the client takes when it detects particular types of commercial applications. The detections include the commercial applications that monitor or record a user's keystrokes or control a user's computer remotely. If a scan detects a commercial keylogger or a commercial remote control program, the client uses the action that is set in the policy. You can also allow the user to control the actions.

Proactive threat scans also detect the processes that behave similarly to adware and spyware. You cannot configure how proactive threat scans handle these types of detections. If proactive threat scans detect the adware or the spyware that you want to allow on your client computers, you should create a centralized exception.

See "Configuring a Centralized Exceptions Policy" on page 579.

Table 31-1 describes the processes that proactive threat scans detect.

Table 31-1 Processes detected by TruScan proactive threat scans

Type of processes	Description
Trojan horses and worms	Processes that exhibit the characteristics of Trojan horses or worms. Proactive threat scans use heuristics to look for the processes that behave like Trojan horses or worms. These processes may or may not be threats. See "Specifying the actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers" on page 530.
Keyloggers	Processes that exhibit the characteristics of keyloggers. Proactive threat scans detect commercial keyloggers, but they also detect any unknown processes that exhibit keylogger behavior. Keyloggers are the keystroke logging applications that capture users' keystrokes. These applications can be used to gather information about passwords and other vital information. They may or may not be threats. See "Specifying the actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers" on page 530.
Commercial applications	Known commercial applications that might be used for malicious purposes. Proactive threat scans detect several different types of commercial applications. You can configure actions for two types: keyloggers and remote control programs. See "Specifying actions for commercial application detections" on page 531.
Adware and spyware	Processes that exhibit the characteristics of adware and spyware Proactive threat scans uses heuristics to detect the unknown processes that behave like adware and spyware. These processes may or may not be risks.

See "Specifying the types of processes that TruScan proactive threat scans detect" on page 529.

You can configure whether or not the client software sends information about proactive threat detections to Symantec. You include this setting as part of an Antivirus and Antispyware Policy.

See "Submitting information about scans to Symantec" on page 422.

About managing false positives detected by TruScan proactive threat scans

TruScan proactive threat scans sometimes return false positives. Proactive threat scans look for applications and processes with suspicious behavior rather than known viruses or security risks. By their nature, these scans typically flag the items that you might not want to detect.

For the detection of Trojan horses, worms, or keyloggers, you can choose to use the default action and sensitivity levels that Symantec specifies. Or you can choose to manage the detection actions and sensitivity levels yourself. If you manage the settings yourself, you risk the detection of many false positives. If you want to manage the actions and sensitivity levels, you should be aware of the impact on your security network.

Note: If you change the sensitivity level, you change the total number of detections. If you change the sensitivity level, you might reduce the number of false positives that proactive threat scans produce. Symantec recommends that if you change the sensitivity levels, you change them gradually and monitor the results.

If a proactive threat scan detects a process that you determine is not a problem, you can create an exception. An exception ensures that future scans do not flag the process. Users on client computers can also create exceptions. If there is a conflict between a user-defined exception and an administrator-defined exception, the administrator-defined exception takes precedence.

See "Configuring a Centralized Exceptions Policy" on page 579.

Table 31-2 outlines the tasks for creating a plan to manage false positives.

Table 31-2 Plan for managing false positives

Task	Description
Ensure that Symantec manages Trojan horse, worm, and keylogger detections.	Antivirus and Antispyware Policies include the Symantec-managed settings. The setting is enabled by default. When this setting is enabled, Symantec determines the actions that are taken for the detections of these types of processes. Symantec also determines the sensitivity level that is used to scan for them. When Symantec manages the detections, proactive threat scans perform an action that is based on how the scan interprets the detection. The scan applies one of the following actions to the detection: ■ Quarantine The scan uses this action for the detections that are likely to be true threats. ■ Log only The scan uses this action for the detections that are likely to be false positives. **Note:** If you choose to manage the detection action, you choose one action. That action is always used for that detection type. If you set the action to Quarantine, the client quarantines all detections of that type.
Ensure that Symantec content is current.	Verify that the computers that produce false positives have the latest Symantec content. The latest content includes information about processes that Symantec has determined to be known false positives. These known false positives are excluded from proactive threat scan detection. You can run a report in the console to check which computers are running the latest version of the content. See "Monitoring endpoint protection" on page 191. You can update the content by doing any of the following actions: ■ Apply a LiveUpdate Policy. See "About LiveUpdate Policies" on page 142. ■ Run the Update command for the selected computers that are listed on the Clients tab. ■ Run the Update command on the selected computers that are listed in the computer status or risk log

Table 31-2 Plan for managing false positives *(continued)*

Task	Description
Make sure that submissions are enabled.	Submissions settings are included as part of the Antivirus and Antispyware Policy. Make sure that client computers are configured to automatically send information to Symantec Security Response about processes detected by proactive threat scans. The setting is enabled by default. See "Submitting information about scans to Symantec" on page 422.
Create exceptions for the false positives that you discover.	You can create a policy that includes exceptions for the false positives that you discover. For example, you might run a certain process or application in your security network. You know that the process is safe to run in your environment. If TruScan proactive threat scans detect the process, you can create an exception so that future scans do not detect the process. See "Configuring a Centralized Exceptions Policy" on page 579.

About the processes that TruScan proactive threat scans ignore

TruScan proactive threat scans allow certain processes and exempt those processes from the scans. Symantec maintains this list of processes. Symantec typically populates the list with the applications that are known false positives. The client computers in your security network receive updates to the list periodically when they download new content. The client computers can download the content in several ways. The management server can send updated content. You or your users can also run LiveUpdate on the client computers.

TruScan proactive threat scans ignore some processes. These processes might include the applications for which Symantec does not have enough information or the applications that load other modules.

You can also specify that TruScan proactive threat scans ignore certain processes. You specify that proactive threat scans ignore certain processes by creating a centralized exception.

Users on client computers can also create exceptions for proactive threat scans. If an administrator-defined exception conflicts with a user-defined exception, proactive threat scans apply only the administrator-defined exception. The scan ignores the user exception.

See "How TruScan proactive threat scans work with centralized exceptions" on page 526.

How TruScan proactive threat scans work with Quarantine

You can configure proactive threat scans to quarantine detections. Users on client computers can restore quarantined items. The Symantec Endpoint Protection client can also restore quarantined items automatically.

When a client receives new definitions, the client rescans quarantined items. If the quarantined items are considered malicious, the client logs the event.

Periodically, client computers receive updates to Symantec-defined lists of known good processes and applications. When new lists are available on client computers, quarantined items are checked against the latest lists. If the latest lists permit any of the quarantined items, the client automatically restores the items.

In addition, administrators or users might create exceptions for proactive threat detections. When the latest exceptions permit the quarantined items, the client restores the items.

Users can view the quarantined items on the View Quarantine page in the client.

The client does not submit the items that proactive threat scans quarantine to a central Quarantine Server. Users can automatically or manually submit items in the local Quarantine to Symantec Security Response.

See "Submitting quarantined items to Symantec" on page 427.

How TruScan proactive threat scans work with centralized exceptions

You can create your own exception lists for the Symantec Endpoint Protection client to check when it runs proactive threat scans. You create these lists by creating exceptions. The exceptions specify the process and the action to take when a proactive threat scan detects a specified process. You can only create exceptions for the processes that are not included in the Symantec-defined list of known processes and applications.

For example, you might want to create an exception to do any of the following:

- Ignore a certain commercial keylogger
- Quarantine a particular application that you do not want to run on client computers

- Allow a specific remote control application to run

To avoid conflicts between exceptions, proactive threat scans use the following order of precedence:

- Symantec-defined exceptions
- Administrator-defined exceptions
- User-defined exceptions

The Symantec-defined list always takes precedence over administrator-defined exceptions. Administrator-defined exceptions always take precedence over user-defined exceptions.

You can use a Centralized Exceptions Policy to specify that known, detected processes are allowed by setting the detection action to Ignore. You can also create a centralized exception to specify that certain processes are not permitted by setting the action to Quarantine or Terminate.

Administrators can force a proactive threat detection by creating a centralized exception that specifies a file name for proactive threat scans to detect. When the proactive threat scan detects the file, the client logs the instance. Because file names are not unique, multiple processes might use the same file name. You can use forced detections to help you create exceptions to ignore, quarantine, or terminate a particular process.

When a proactive threat scan on the client computer logs the detection, the detection becomes part of a list of known processes. You can select from the list when you create an exception for proactive threat scans. You can set a particular action for the detection. You can also use the proactive detection log under the Monitors tab in the console to create the exception.

See "Configuring a Centralized Exceptions Policy" on page 579.

See "Viewing logs" on page 267.

Users can create exceptions on the client computer through one of the following methods:

- The View Quarantine list
- The scan results dialog box
- Centralized exceptions

An administrator can lock an exceptions list so that a user cannot create any exceptions. If a user previously created exceptions before the administrator locked the list, the user-created exceptions are disabled.

Understanding TruScan proactive threat detections

When a TruScan proactive threat scan detects processes that it flags as potentially malicious, typically some of the processes are legitimate processes. Some detections do not provide enough information to be categorized as a threat or a false positive; these processes are considered "unknown."

A proactive threat scan looks at the behavior of active processes at the time that the scan runs. The scan engine looks for behavior such as opening ports or capturing keystrokes. If a process involves enough of these types of behaviors, the scan flags the process as a potential threat. The scan does not flag the process if the process does not exhibit suspicious behavior during the scan.

By default, proactive threat scans detect the processes that behave like Trojan horses and worms or processes that behave like keyloggers. You can enable or disable these types of detections in an Antivirus and Antispyware Policy.

Note: Proactive threat scan settings have no effect on antivirus and antispyware scans, which use signatures to detect known risks. The client detects known risks first.

See "Specifying the types of processes that TruScan proactive threat scans detect" on page 529.

The client uses Symantec default settings to determine what action to take on the detected items. If the scan engine determines that the item does not need to be remediated, the client logs the detection. If the scan engine determines that the item should be remediated, the client quarantines the item.

Note: The **Scan for trojans and worms** and the **Scan for keyloggers** options are currently not supported on Windows server operating systems or 64-bit Windows XP Professional. The **Scan for keyloggers** option is also not supported on Windows 7. You can modify the options in the Antivirus and Antispyware Policy for the clients that run on server operating systems, but the scans do not run. In the client user interface on server operating systems, the scanning options appear unavailable. If you enable the scanning options in the policy, the options are checked and unavailable.

Symantec default settings are also used to determine the sensitivity of the proactive threat scan. When the sensitivity level is higher, more processes are flagged. When the sensitivity level is lower, fewer processes are flagged. The sensitivity level does not indicate the level of certainty about the detection. It also

does not affect the rate of false positive detections. The higher the sensitivity level, the more false positives and true positives the scan detects.

You should use the Symantec default settings to help minimize the number of false positives that you detect.

You can disable the Symantec-defined default settings. When you disable the Symantec default settings, you can configure actions and the sensitivity level for the detection of Trojan horses, worms, or keyloggers. In the client user interface, the default settings that appear do not reflect the Symantec default settings. They reflect the default settings that are used when you manually manage detections.

For commercial applications, you can specify the action that the client takes when a proactive threat scan makes a detection. You can specify separate actions for the detection of a commercial keylogger and the detection of a commercial remote control application.

See "Specifying the actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers" on page 530.

See "Specifying actions for commercial application detections" on page 531.

Note: Users on client computers can modify the proactive threat scan settings if the settings are unlocked in the Antivirus and Antispyware Policy. On the client computer, the TruScan proactive threat scan settings appear under Proactive Threat Protection.

Specifying the types of processes that TruScan proactive threat scans detect

By default, TruScan proactive threat scans detect Trojan horses, worms, and keyloggers. You can disable the detection of Trojan horses and worms, or keyloggers.

See "Understanding TruScan proactive threat detections" on page 528.

You can click Help for more information about the scan's process type options.

To specify the types of processes that TruScan proactive threat scans detect

1. On the Antivirus and Antispyware Policy page, click **TruScan Proactive Threat Scans**.
2. On the Scan Details tab, under Scanning, check or uncheck **Scan for trojans and worms** and **Scan for keyloggers**.
3. Click **OK**.

Specifying the actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers

TruScan proactive threat scans differ from antivirus and antispyware scans. Antivirus and antispyware scans look for known risks. Proactive threat scans look for unknown risks based on the behavior of certain types of processes or applications. The scans detect any behavior that is similar to the behavior of Trojan horses, worms, or keyloggers.

See "Understanding TruScan proactive threat detections" on page 528.

When you let Symantec manage the detections, the detection action is Quarantine for true positives and Log only for false positives.

When you manage the detections yourself, you can configure the detection action. That action is always used when proactive threat scans make a detection. For example, you might specify that the Symantec Endpoint Protection client logs the detection of processes that behave like Trojan horses and worms. When the client makes a detection, it does not quarantine the process, it only logs the event.

You can configure the sensitivity level. Proactive threat scans make more detections (true positives and false positives) when you set the sensitivity level higher.

Note: If you enable these settings, you risk detecting many false positives. You should be aware of the types of processes that you run in your security network.

You can click Help for more information about the scan's action and sensitivity options.

To specify the action and sensitivity for Trojan horses, worms, or keyloggers

1. On the Antivirus and Antispyware Policy page, click **TruScan Proactive Threat Scans**.
2. On the Scan Details tab, under Scanning, make sure that you check **Scan for trojans and worms** and **Scan for keyloggers**.
3. For either risk type, uncheck **Use defaults defined by Symantec**.
4. For either risk type, set the action to Log, Terminate, or Quarantine.

   Notifications are sent if an action is set to Quarantine or Terminate, and you have enabled notifications. (Notifications are enabled by default.) Use the Terminate action with caution. In some cases, you can cause an application to lose functionality.
5. Do one of the following actions:

- Move the slider to the left or right to decrease or increase the sensitivity, respectively.
- Click **Low** or **High**.

6 Click **OK**.

Specifying actions for commercial application detections

You can change the action that is taken when a TruScan proactive threat scan makes a detection. If you set the action to Ignore, proactive threat scans ignore commercial applications.

See "Understanding TruScan proactive threat detections" on page 528.

You can click Help for more information about the options that are used in procedures.

To specify actions for commercial application detections

1 On the Antivirus and Antispyware Policy page, click **TruScan Proactive Threat Scans**.

2 On the Scan Details tab, under Detecting Commercial Applications, set the action to Ignore, Log, Terminate, or Quarantine.

3 Click **OK**.

Configuring the TruScan proactive threat scan frequency

You can configure how often TruScan proactive threat scans run by including the setting in an Antivirus and Antispyware Policy.

Note: If you change the frequency of proactive threat scans, it can impact the performance of client computers.

See "About TruScan proactive threat scans" on page 519.

You can click Help for more information about the scan's frequency options.

To configure the proactive threat scan frequency

1 On the Antivirus and Antispyware Policy page, click **TruScan Proactive Threat Scans**.

2 On the Scan Frequency tab, under Scan Frequency, set one of the following options:

- At the default scanning frequency
  The scan engine software determines the scan frequency. This option is the default setting.
- At a custom scanning frequency
  If you enable this option, you can specify that the client scans new processes immediately when it detects them. You can also configure the scan frequency time.

3 Click **OK**.

Configuring notifications for TruScan proactive threat scans

By default, notifications are sent to client computers whenever there is a TruScan proactive threat scan detection. You can disable notifications if you do not want the user to be notified.

See "About TruScan proactive threat scans" on page 519.

Notifications alert the user that a proactive threat scan made a detection that the user should remediate. The user can use the **Notifications** dialog box to remediate the detection. Some proactive threat scan detections do not require remediation. For these detections, the Symantec Endpoint Protection client logs the detection but does not send a notification.

Note: If you set the detections to use the Symantec default settings, notifications are sent only if the client recommends a remediation for the process.

Users can also remediate detections by viewing the Threat log and by selecting an action.

You can create a centralized exception to exclude a process from detection; users on client computers can also create exceptions.

See "About Centralized Exceptions Policies" on page 575.

You can click **Help** for more information about the scan's notification options.

To configure notifications for TruScan proactive threat scans

1 On the **Antivirus and Antispyware Policy** page, click **TruScan Proactive Threat Scans**.

2 On the **Notifications** tab, check or uncheck the following options:

- **Display a message when there is a detection**

- **Prompt before terminating a process**
- **Prompt before stopping a service**

3 Click **OK**.

Chapter 32

Configuring application and device control

This chapter includes the following topics:

About application and device control

You might want to use application and device control for the following reasons:

- To prevent malware from hijacking applications on client computers
- To prevent the inadvertent removal of data from client computers
- To restrict the applications that can run on a client computer
- To minimize the possibility of a computer being infected with security threats from a peripheral device

Application and device control is implemented on client computers using an Application and Device Control Policy.

An Application and Device Control Policy offers the following types of protection for client computers:

- Application control to monitor the Windows API calls made on client computers and to control access to clients' files, folders, Windows registry keys, and processes.
  It protects system resources from applications.
  See "About application control" on page 537.
- Device control to manage the peripheral devices that can attach to computers.
  See "About device control" on page 542.

You can define each of these two types of protection when you create a new Application and Device Control Policy. You also have the option to add either application control or device control first and then the other type of protection at a later time.

See "About the structure of an Application and Device Control Policy" on page 536.

You can apply only one Application and Device Control Policy to each location within a group. You must define both application control and device control in the same policy if you want to implement both types of protection.

See "About working with Application and Device Control " on page 543.

Note: The information in this chapter applies only to 32-bit client computers. Application and Device Control Policies do not work on 64-bit client computers.

About the structure of an Application and Device Control Policy

The application control portion of an Application and Device Control Policy can contain multiple rule sets, and each rule set contains one or more rules. You can configure properties for a rule set, and properties, conditions, and actions for each rule.

Rules control attempts to access computer entities, such as files or Windows registry keys, that Symantec Endpoint Protection monitors. You configure these different types of attempts as conditions. For each condition, you can configure actions to take when the condition is met. You configure rules to apply to only certain applications, and you can optionally configure them to exclude other applications from having the action applied.

See “About application control rule properties” on page 540.

See “About application control rule conditions” on page 540.

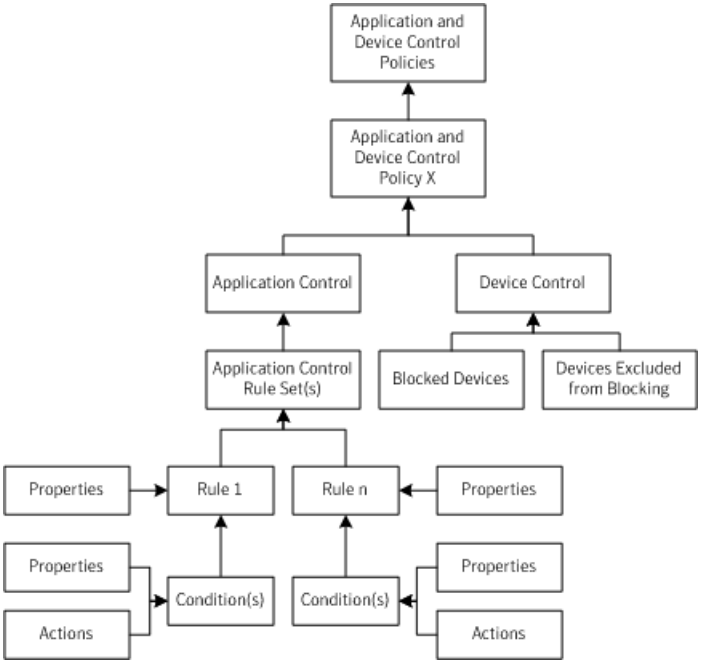
See “About application control rule condition properties” on page 541.

See “About application control rule condition actions” on page 541.

Device control consists of a list of blocked devices and a list of devices that are excluded from blocking. You can add to these two lists and manage their contents.

Figure 32-1 illustrates the application and device control components and how they relate to each other.

Figure 32-1 Application and Device Control Policy structure



About application control

Application control provides the ability to monitor and to control the behavior of applications. You can block or allow access to specified Windows registry keys, files, and folders. You can also block or allow applications to launch or terminate other processes. You can define which applications are permitted to run and which applications cannot be terminated through irregular processes. You can define which applications can call Dynamic Link Libraries (DLLs).

Warning: Application control is an advanced security feature that only experienced administrators should configure.

Application control is implemented by using sets of rules that define how you want to control the applications. Application control is a set of controls that allow or block an action. You can create as many rule sets as you need in a policy. You can also configure which rule sets are active at any given time by using the Enabled option for each rule set.

You can use application control to protect client computers in the following ways:

- Protect specific Windows registry keys and values.
- Safeguard directories such as the \WINDOWS\system directory.
- Prevent users from altering configuration files.
- Shield important program files such as the Symantec home directory where the client is installed.
- Protect specific processes or exclude processes from protection.
- Control access to DLLs.

See "Creating an Application and Device Control Policy" on page 545.

See "About Test mode" on page 538.

See "About application control rule sets and rules" on page 539.

About Test mode

When you create an application control rule set, you create it in the default mode, which is Test (log only) mode. Test mode lets you test your rules before you enable them. In Test mode, no actions are applied, but the actions that you have configured are logged as if they had been applied. Using Test mode, you can assign the policy to groups and locations and generate a client Control log. Examine the client Control logs for errors and make corrections to the rule as necessary. When the policy operates as you expect it to, you can change the mode to Production mode to implement the application control rule set.

A best practice is to run all rule sets in Test mode for a period of time before you switch them to Production mode. This practice reduces the potential for the problems that can occur when you do not anticipate all the possible ramifications of a rule.

See "Changing the mode of an application control rule set" on page 555.

About application control rule sets and rules

Rule sets consist of rules and their conditions. A rule is a set of conditions and actions that apply to a given process or processes. A best practice is to create one rule set that includes all of the actions that allow, block, and monitor one given task. Follow this principle to help to keep your rules organized. For example, suppose you want to block write attempts to all removable drives and you want to block applications from tampering with a particular application. To accomplish these goals, you should create two different rule sets. You should not create all of the necessary rules to accomplish both these goals with one rule set.

Note: Currently, Symantec Endpoint Protection Manager does not support a rule set that specifies the blocking of write attempts to CD or DVD drives. You can select the option in the Application and Device Control Policy, however, the option is not enforced. Instead, you can create an Application and Device Control Policy that blocks specific applications that write to CD or DVD drives. You should also create a Host Integrity Policy that sets the Windows registry key to block write attempts to CD or DVD drives.

For the latest information, see the Symantec Knowledge Base document: After setting up an Application and Device Control policy to block CD writing, CD writing is not blocked as expected, and write attempt is not logged.

You apply a rule to one or more applications to define the applications that you monitor. Rules contain conditions. These conditions monitor the application or applications that are defined in the rule for specified operations. Conditions define what you want to allow the applications to do or to keep them from doing. Conditions also contain the actions to take when the operation that is specified in the condition is observed.

Note: Remember that actions always apply to the process that is defined in the rule. They do not apply to the processes that are defined in the condition.

See "Creating a new application control rule set and adding a new rule to the set" on page 547.

See "About application control rule properties" on page 540.

See "About application control rule conditions" on page 540.

See "About application control rule condition properties" on page 541.

See "About application control rule condition actions" on page 541.

About application control rule properties

You can configure the following properties for a rule:

- A name
- A description (optional)
- Whether the rule is enabled or disabled
- A list of the applications that should have the rule applied to them
- A list of the applications that should not have the rule applied to them (optional)

See "About the structure of an Application and Device Control Policy" on page 536.

About application control rule conditions

Conditions are the operations that can be allowed or denied for applications.

Table 32-1 describes the application control rule conditions that you can configure for a rule.

Table 32-1 Types of rule conditions

Condition	Description
Registry Access Attempts	Allow or block access to a client computer's Windows registry settings. You can allow or block access to specific Windows registry keys, values, and data.
File and Folder Access Attempts	Allow or block access to specified files or folders on a client computer. You can restrict the monitoring of files and folders to specific drive types.
Launch Process Attempts	Allow or block the ability to launch a process on a client computer.
Terminate Process Attempts	Allow or block the ability to terminate a process on a client computer. For example, you may want to block a particular application from being stopped. This condition looks for the applications that try to kill a specified application. **Note:** This condition prevents other applications or procedures from terminating the process. It does not prevent application termination by the usual methods of quitting an application, such as clicking Quit from the File Menu.

Table 32-1 Types of rule conditions *(continued)*

Condition	Description
Load DLL Attempts	Allow or block the ability to load a DLL on a client computer. You can define the DLL files that you want to prevent or allow to be loaded into an application. You can use specific file names, wildcard characters, fingerprint lists, and regular expressions. You can also limit the monitoring of DLLs to those DLLs that are launched from a particular drive type.

See "About the structure of an Application and Device Control Policy" on page 536.

See "Adding conditions to a rule" on page 548.

See "Configuring condition properties for a rule" on page 549.

See "Configuring the actions to take when a condition is met" on page 551.

About application control rule condition properties

You can configure the following properties for a rule condition:

- A name
- A description (optional)
- Whether the rule condition is enabled or disabled
- A list of the computer entities that should be monitored for the condition
- A list of the computer entities that should be excluded from monitoring for the condition (optional)

See "About the structure of an Application and Device Control Policy" on page 536.

About application control rule condition actions

You can configure certain actions to be taken when a condition is met.

The following actions can be configured when an application attempt occurs:

- Continue processing other rules.
- Allow the application to access the entity.
- Block the application from accessing the entity.
- Terminate the application process.

For example, you can configure one set of actions to take place when a process tries to read a monitored entity. You can configure a different set of actions to

occur when the same process tries to create, delete, or write to a monitored entity. You can configure an action in each case for as many processes as you want.

You can also configure application control to log the attempts and to display a custom message to the user when an attempt has occurred.

Warning: Use the Terminate process action carefully because it may not have the effect that you expect when you use it in a rule. It terminates the process that is performing the configured action, not the process that the user is currently starting.

For example, suppose you want to terminate Winword.exe any time that any process launches Winword.exe. You decide to create a rule, and you configure it with the Launch Process Attempts condition and the Terminate process action. You apply the condition to Winword.exe and apply the rule to all processes. One may expect this rule to terminate Winword.exe, but that is not what a rule with this configuration does. If you try to start Winword.exe from Windows Explorer, a rule with this configuration terminates Explorer.exe, not Winword.exe.

See "About the structure of an Application and Device Control Policy" on page 536.

About device control

Use device control to manage peripheral devices' access to client computers. Device control gives an administrator a finer level of control over the devices that are allowed to access computers. You can construct a list of devices that should be blocked from computer access and a list of devices that should be allowed access. Although a device might be physically connected to a computer, the device can still be denied access to that computer. You can block or allow USB, infrared, FireWire, and SCSI devices, as well as serial ports and parallel ports. You can also allow other device types (such as a USB hard drive) to be excluded from being blocked. You can also choose to define device control by using either the Windows GUID or the device ID. You can implement device control by constructing hardware device lists.

Table 32-2 lists sample port and device configuration combinations and the effect each combination has on the device that tries to access the client computer.

Table 32-2 Port and device configuration combinations

Configuration	Result
Port blocked + device excluded	Device works

Table 32-2 Port and device configuration combinations *(continued)*

Configuration	Result
Port excluded + device blocked	Device does not work **Note:** You should never block a keyboard.

For example, you may decide to block all ports, but exclude a USB mouse so that it can connect to a client computer. In this scenario, the USB mouse works on the client computer even though that port is blocked.

See "About application and device control" on page 535.

See "Configuring device control for an Application and Device Control Policy" on page 556.

About working with Application and Device Control

By default, there is an Application and Device Control Policy on the management server. However, by default the Application and Device Control Policy driver is disabled on the client. To enable the driver, you must either enable an existing rule or add and enable a new rule in the policy. After the policy is downloaded to the client computer, a notification requests that the user restart the client computer. The user must restart the client to enable the policy to protect the client computer.

If the default Application and Device Control Policy does not provide the protection you need, you have the following choices:

- Edit the default policy.
- Create a custom policy.

See "Configuring application control for an Application and Device Control Policy" on page 546.

If you withdraw or disable the Application and Device Control Policy, the driver is disabled and the client is not protected. To enable protection again, the user has to restart the client computer again.

Warning: An Application and Device Control Policy is a powerful tool that lets you create custom enforcement policies for your environment. However, configuration errors can disable a computer or a server. The client computer can fail, or its communication with the Symantec Endpoint Protection Manager can be blocked, when you implement an Application and Device Control Policy. If this type of failure occurs, you may not be able to configure the client computer remotely. Your only option may be to restore the client computer locally. Symantec recommends you first use a policy in Test mode before you deploy it. You can then examine the Control log for errors.

Application and device control events are recorded in the client's Control log. You can view them on the console in the Application Control log and the Device Control log.

Enabling a default application control rule set

The application control portion of an Application and Device Control Policy is made up of application control rule sets. Each application control rule set is made up of one or more rules. Default application control rule sets are installed with the Symantec Endpoint Protection Manager. The default rule sets are disabled at installation.

Note: Do not edit the default application control rule sets. If the default rule sets and controls do not meet your requirements, create a new application control rule set to meet your requirements instead.

If you want to use the default rule sets in an Application and Device Control Policy, you must enable them.

See "About application control rule sets and rules" on page 539.

To enable a default application control rule set

1. In the Console, click **Policies**.
2. Under View Policies, click **Application and Device Control**.
3. In Application and Device Control Policies pane, click the policy to which you want to add a default application control rule set.
4. Under Tasks, click **Edit the Policy**.
5. In the Application and Device Control Policy pane, click **Application Control**.

6 To review the setting in a default application control rule set, click the name under Rule Set, and then click **Edit**.

Be sure not to make any changes.

7 When you have finished reviewing the rules and their condition settings, click **Cancel**.

8 Check the check box next to each rule set that you want to enable.

9 Click **OK**.

Creating an Application and Device Control Policy

You can create a new Application and Device Control Policy. After you create a new policy, you can create one or more application control rule sets, or hardware device control lists, or both.

You should not create one policy that contains only device control and one that contains only application control. An Application and Device Control Policy must contain both application control and device control if you want to implement both. You can only assign one Application and Device Control Policy at a time to a group or a location.

See "About the structure of an Application and Device Control Policy" on page 536.

To create and assign an Application and Device Control Policy

1 In the Symantec Endpoint Protection Manager Console, click **Policies**.

2 Under View Policies, click **Application and Device Control**.

3 Under Tasks, click **Add an Application and Device Control Policy**.

4 In the Overview pane, in the Policy name field, type the name of the new Application and Device Control Policy.

The default name for a new policy is New Application and Device Control Policy.

5 In the Description field, type a description of the new policy.

This information is optional; it is used for reference purposes only.

6 If you do not want to immediately implement the policy, uncheck **Enable this policy**.

New policies are enabled by default.

7 Click **OK**.

See "Configuring application control for an Application and Device Control Policy" on page 546.

See "Configuring device control for an Application and Device Control Policy" on page 556.

Configuring application control for an Application and Device Control Policy

To configure application control, you need to accomplish the following tasks:

- Create a new application control rule set.
  See "Creating a new application control rule set and adding a new rule to the set" on page 547.
- Add one or more rules to the rule set.
  See "Creating a new application control rule set and adding a new rule to the set" on page 547.
- Add one or more conditions to the rules.
  See "Adding conditions to a rule" on page 548.
  See "Configuring condition properties for a rule" on page 549.
- Configure the actions to be taken when the conditions are met.
  See "Configuring the actions to take when a condition is met" on page 551.
- Apply the conditions to entities.
  See "Applying a rule to specific applications and excluding applications from a rule" on page 552.
- Optionally, exclude entities from having the conditions applied to them.
  See "Applying a rule to specific applications and excluding applications from a rule" on page 552.
- Apply the rules to processes.
  See "Applying a rule to specific applications and excluding applications from a rule" on page 552.
- Optionally, exclude processes from having the rules applied to them.
  See "Applying a rule to specific applications and excluding applications from a rule" on page 552.

- Enable the rules.
  See "Creating a new application control rule set and adding a new rule to the set" on page 547.
- Enable the rule set.
  See "Enabling a default application control rule set" on page 544.
  See "Disabling application control rule sets and individual rules in an Application and Device Control Policy" on page 554.

Creating a new application control rule set and adding a new rule to the set

A new application rule set contains one or more administrator-defined rules. Each rule set and each rule has properties. Each rule can also contain one or more conditions for monitoring applications and their access to specified files, folders, Windows registry keys, and processes.

You can create multiple rules and add them to a single application control rule set. Create as many rules and as many rule sets as you need to implement the protection you want. You can delete rules from the rules list and change their position in the rule set hierarchy as needed. You can also enable and disable rule sets or individual rules within a set.

The order in which the rules are listed is important to the functioning of application control. Application control rules work similarly to most network-based firewall rules in that both use the first rule match feature. When there are multiple rules where the conditions are true, the top rule is the only one that is applied unless the action that is configured for the rule is to Continue processing other rules.

You should consider the order of the rules and their conditions when you configure them to avoid unexpected consequences. Consider the following scenario: Suppose an administrator wants to prevent all users from moving, copying, and creating files on USB drives. The administrator has an existing rule with a condition that allows write access to a file named Test.doc. The administrator adds a second condition to this existing rule set to block all USB drives. In this scenario, users are still able to create and modify a Test.doc file on USB drives. Because the Allow write access to Test.doc condition comes before the Block write access to USB drives condition in the rule, the Block write access to USB drives condition does not get processed when the condition that precedes it in the list is true.

You can review the structure of the default rule sets to see how they are constructed.

Warning: Only advanced administrators should create application control rule sets.

Configuration errors in the rule sets that are used in an Application and Control Policy can disable a computer or a server. The client computer can fail, or its communication with the Symantec Endpoint Protection Manager can be blocked.

To create a new rule set and add rules to it

1. Create a new Application and Device Control Policy.

   See "Adding a shared policy" on page 94.

2. In the Application Control pane, click **Add**.
3. In the Add Application Control Rule Set dialog box, uncheck **Enable logging** if you do not want to log events about this rule set.

   Logging is enabled by default.

4. In the Rule set name text box, change the default name for the rule set.
5. In the Description field, type a description.
6. Change the default name for the rule in the Rule name text box, and then type a description of the rule.
7. If you do not want to immediately enable this new rule, uncheck **Enable this rule**.
8. To add a second rule, click **Add**, and then click **Add Rule**.
9. Click **OK**.

   After you create a rule set and a rule, you should define the applications that the rule should apply to. If necessary, you should also define any applications that should be excluded from having the rule applied to them. You can then add conditions to the rule and configure actions to be taken when the conditions are met.

   See "Applying a rule to specific applications and excluding applications from a rule" on page 552.

Adding conditions to a rule

After you apply a rule to at least one application, you can add and configure conditions for the rule. Conditions have properties and actions. A condition's properties specify what the condition looks for. Its actions define what happens when the condition is met.

See "Configuring application control for an Application and Device Control Policy" on page 546.

To add a condition to a rule

1. In the Application Control pane, click the rule set you created, and then click **Edit**.
2. In the Edit Application Control Rule Set dialog box, click the rule to which you want to add a condition.
3. Under the Rules list, click **Add**, and then click **Add Condition**.
4. Select one of the following conditions:
   - Registry Access Attempts
   - File and Folder Access Attempts
   - Launch Process Attempts
   - Terminate Process Attempts
   - Load DLL Attempts

   You can add, configure, and delete conditions from a rule as needed.

Configuring condition properties for a rule

Condition properties include the name, description, and whether the condition is enabled or disabled. Condition properties also include the application of the condition to entities and optionally, the exclusion of some entities from having the condition applied.

Note: When you apply a condition to all entities in a particular folder, a best practice is to use *folder_name** or *folder_name***. One asterisk includes all the files and folders in the named folder. Use *folder_name*** to include every file and folder in the named folder plus every file and folder in every subfolder.

See "Configuring application control for an Application and Device Control Policy" on page 546.

To configure condition properties

1. In the Edit Application Control Rule Set dialog box, click the condition that you want to apply.
2. If desired, change the default name in the Name text box, and optionally add a description.
3. If you want to immediately enable this condition, check **Enable this condition**.

4 To the right of Apply to the following *entity*, where *entity* represents processes, Windows registry keys, files and folders, or DLLs, click **Add**.

5 In the Add *entity* Definition dialog box, configure one of the following sets of options:

- For **Registry Access Attempts**, type the name of the Windows registry key and its value name and data.
  Click either **Use wildcard matching (* and ? supported)** or **Use regular expression matching**.
- For **File and Folder Access Attempts**, type the name of the file or folder.
  Click either **Use wildcard matching (* and ? supported)** or **Use regular expression matching**.
  If desired, check specific drive types on which to match the files and folders.
  If desired, check **Only match files running on the following device id type**, and then type a device ID type in the text field or click **Select** to select a device ID type from the list in the Device Selection dialog box to only match the processes that run on devices of that ID type.
- For **Launch Process Attempts**, type the name of the process.
  Click either **Use wildcard matching (* and ? supported)** or **Use regular expression matching**.
  If desired, check specific drive types on which to match the process.
  If desired, check **Only match processes running on the following device id type**, and then type a device ID type in the text field or click **Select** to select a device ID type from the list in the Device Selection dialog box to only match the processes that run on devices of that ID type.
  If desired, click **Options** to match processes based on the file fingerprint and to only match the processes that have a designated argument. You can choose to match the arguments exactly or by using regular expression matching.
- For **Terminate Process Attempts** or **Load DLL Attempts**, type the name of the process.
  Click either **Use wildcard matching (* and ? supported)** or **Use regular expression matching**.
  If desired, check specific drive types on which to match the process.
  If desired, check **Only match processes running on the following device id type**, and then type a device ID type in the text field or click **Select** to select a device ID type from the list in the Device Selection dialog box to only match the processes that run on devices of that ID type.
  If desired, click **Options** to match processes based on the file fingerprint.

6 Click **OK**.

7 To the right of the Do not apply this rule to the following processes pane, click **Add**, and repeat the configuration as desired.

You have the same options for the exclusions as you do for the inclusions.

8 Click the appropriate controls to make your selections, and type any required information into the text boxes.

9 Click **OK**.

After you set properties for the condition, you need to configure the actions that are taken when the condition is met.

See "Configuring the actions to take when a condition is met" on page 551.

Configuring the actions to take when a condition is met

The following actions are available for all conditions:

Continue processing other rules	Allows you to only log the event and then continue processing other rules in the list For all other actions, the client computer stops processing rules after the first criterion matches
Allow access	Allows the operation to continue
Block access	Prevents the operation
Terminate Process	Kills the application that has made the request

Note: A best practice is to use the Block access action to prevent a condition rather than to use the Terminate process action. The Terminate process action should be used only in advanced configurations.

See "Configuring application control for an Application and Device Control Policy" on page 546.

To configure the actions to take when a condition is met

1 In the Edit Application Control Rule Set dialog box, click the condition for which you want to configure actions.

2 On the Actions tab, do one of the following actions:

- For the Launch Process Attempts condition and the Terminate Process Attempts condition, click one of the following options: **Continue processing other rules**, **Allow access**, **Block access**, or **Terminate process**.

- For the DLL Access Attempts condition, click one of the following options: **Continue processing other rules**, **Allow access**, **Block access**, or **Terminate process**.
- For the Registry Access Attempts condition and the File and Folder Access Attempts condition, you can configure two sets of actions. One set applies when there is a read attempt; the other set applies when there is a create, delete, or write attempt.
  Under Read Attempt, click one of the following options: **Continue processing other rules**, **Allow access**, **Block access**, or **Terminate process**.

3. If desired, check **Enable logging**, and then select a severity level to assign to the entries that are logged.
4. If desired, check **Notify user**, and then type the text that you want to user to see.
5. Repeat steps 2 through 4 to configure the same options for Create, Delete, or Write Attempts.
6. Click **OK**.

Applying a rule to specific applications and excluding applications from a rule

You can apply a rule to applications, and you can exclude applications from the rule's actions. You specify one list that contains the applications to which the rule applies (the inclusions). You specify another list that contains the applications to which the rule does not apply (the exclusions). To tie a rule to a specific application, you define that application in the Apply this rule to the following processes text field.

If you want to tie the rule to all applications except for a given set of applications, then you can use the following settings:

- In the Apply this rule to the following processes text box, define a wildcard character for all processes (*).
- In the Do not apply this rule to the following processes text box, list the applications that need an exception.

You can define as many applications as you want for each list.

Note: Every rule must have at least one application listed in the Apply this rule to the following processes text box.

When you add applications to a rule, you can use the following ways to specify the application:

- The process name
- Wildcard characters
- Regular expressions
- File fingerprints
- The drive types from where the application was launched
- The device ID

See "Configuring application control for an Application and Device Control Policy" on page 546.

To apply a rule to specific applications

1. In the Edit Application Control Rule Set dialog box, click the rule that you want to apply.
2. If you want to configure an application to apply the rule to, then to the right of Apply this rule to the following processes, click **Add**.
3. In the Add Process Definition dialog box, configure the following items:
   - Type the name of the application that you want to match in this rule.
   - Click either **Use wildcard matching (* and ? supported)** or **Use regular expression matching** for matching the name.
   - If desired, check the specific drive types on which to match the process.
   - If desired, check **Only match processes running on the following device id type**, and then type a device ID type in the text field or click **Select** to select a device ID type from the list in the Device Selection dialog box to only match the processes that run on devices of that ID type.
   - If desired, click **Options** to match processes based on the file fingerprint and to match only the processes that have a designated argument. You can choose to match the arguments exactly or by using regular expression matching.
4. Click **OK**.

   You can repeat steps 2 through 4 to add as many applications as you want.

5 If you want to configure one or more applications to exclude from the rule, then to the right of the Do not apply this rule to the following processes text field, click **Add**.

Repeat the configuration of the applications to exclude as desired. You have the same options when you define an application to exclude as you have when you apply the rule to an application.

6 When you have finished defining the applications, click **OK**.

Changing the order in which application control rule sets are applied

You can control the order in which application control rule sets are applied. You can also control the order in which individual rules within a rule set are applied.

See "Configuring application control for an Application and Device Control Policy" on page 546.

To change the order in which application control rule sets are applied

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

2 In the View Policies pane, click **Application and Device Control**.

3 Click the policy that you want to edit.

4 Under Tasks, click **Edit the Policy**.

5 Click **Application Control**.

6 Click the application control rule set that you want to move.

7 Click **Move Up** or **Move Down** to change its priority within the list.

8 Repeat the previous two steps for each rule set that you want to reprioritize.

9 Click **OK**.

Disabling application control rule sets and individual rules in an Application and Device Control Policy

You may need to disable a particular application control rule set in an Application and Device Control Policy without withdrawing or deleting the entire policy.

See "Configuring application control for an Application and Device Control Policy" on page 546.

To disable an application control rule set in an Application and Device Control Policy

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

2 Under View Policies, click **Application and Device Control**.

3 Click the policy that contains the rule set that you want to disable.

4 Under Tasks, click **Edit the Policy**.

5 Click **Application Control**.

6 Uncheck the check box next to the rule set that you want to disable.

7 Click **OK**.

You have now disabled a single rule set without disabling the entire policy.

To disable an individual rule in an Application and Device Control Policy

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

2 Under View Policies, click **Application and Device Control**.

3 Click the policy that contains the rule that you want to disable.

4 Under Tasks, click **Edit the Policy**.

5 Click **Application Control**.

6 Click the rule set that contains the rule that you want to disable, and then click **Edit**.

7 Under Rules, in the list of rules, click the rule that you want to disable.

8 On the Properties tab, uncheck **Enable this rule**.

9 In the Edit Application Control Rule Set dialog box, click **OK**.

10 Click **OK**.

You have now disabled a single subordinated rule without disabling the entire policy or rule set.

Changing the mode of an application control rule set

When you first create an application control rule set, you create it in Test mode. After you test the rule set within a policy, then you can change the mode to Production mode.

See "About Test mode" on page 538.

To change the mode of an application control rule set

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

2 Under View Policies, click **Application and Device Control**.

3 Click the policy that contains the application control rule set that you want to change.

4 Click **Edit the Policy**.

5 Click **Application Control**.

6 Click the rule set that you want to change.

7 Under Test/Production, click the corresponding drop-down list arrow to display the list of modes.

8 Click the new mode.

9 Click **OK**.

Configuring device control for an Application and Device Control Policy

Use device control to manage hardware devices. You can modify this list at any time.

See "About device control" on page 542.

See "About hardware devices" on page 557.

To add device control

1 In the Application and Device Control Policy pane, click **Device Control**.

2 Under Blocked Devices, click **Add**.

3 Review the list of hardware devices, and click any device or devices that you want to block from accessing the client computer.

4 Click **OK**.

5 Under Devices Excluded From Blocking, click **Add**.

6 Review the list of hardware devices, and click any devices that you want to exclude from being blocked when they access the client computer.

7 If you do not want device control information to be logged, uncheck **Log blocked devices**.

The information is logged by default.

8 If you want users to be notified, check **Notify users when devices are blocked**.

If you enabled notification, click **Specify Message Text**, and then type the text that you want the users to see.

9 Click **OK**.

Chapter 33

Customizing Application and Device Control Policies

This chapter includes the following topics:

About hardware devices

You can use a default list of hardware devices to add a vendor-specific device to an Application and Device Control Policy. The Hardware Devices list eliminates the need to retype these devices each time you want to add one from a rule.

Two numeric values identify hardware devices: device IDs and class IDs. You can use either of these two values to identify devices on the Hardware Devices list.

See “About device IDs” on page 558.

See “About class IDs” on page 558.

The Symantec Endpoint Protection Manager console includes lists of the devices that can be blocked and the devices that can be excluded from blocking, as needed. An administrator can add devices, delete devices, or edit the devices in the list.

Note: You can neither edit nor delete the default devices.

About class IDs

The class ID refers to the Windows GUID. Each device type has both a Class and a ClassGuid associated with it. The ClassGuid is a hexadecimal value with the following format:

{00000000-0000-0000-0000-000000000000}

See "Obtaining a class ID or device ID" on page 559.

See "About hardware devices" on page 557.

About device IDs

A device ID is the most specific ID for a device. The syntax of a device ID includes some descriptive strings that make it easier to read than the class ID.

When you add a device ID, you can use a device's specific ID. Alternately, you can use a wildcard character in the device ID string to indicate a less specific group of devices. You can use an asterisk (*) to indicate zero or more additional characters or a question mark (?) to indicate a single character of any value.

The following is a device ID for a specific USB SanDisk device:

USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO&REV_2033
\0002071406&0

The following is a device ID with a wildcard that indicates any USB SanDisk device:

USBSTOR\DISK&VEN_SANDISK*

The following is a device ID with a wildcard that indicates any USB disk device:

USBSTOR\DISK*

The following is a device ID with a wildcard that indicates any USB storage device:

USBSTOR*

See "Obtaining a class ID or device ID" on page 559.

See "About hardware devices" on page 557.

Obtaining a class ID or device ID

You can use the Symantec DevViewer tool to obtain either the class ID (GUID) or the device ID. You can use Windows Device Manager to obtain the device ID.

After you obtain a device ID, you can modify it with a wildcard character to indicate a less specific group of devices.

To obtain a class ID or device ID by using the DevViewer tool

1. On your product disc, locate the \TOOLS\NOSUPPORT\DEVVIEWER folder, and then download the DevViewer.exe tool to the client computer.
2. On the client computer, run DevViewer.exe.
3. Expand the Device Tree and locate the device for which you want the device ID or the GUID.
4. In the right-hand pane, right-click the device ID (it starts with [device id]), and then click **Copy Device ID**.
5. Click **Exit**.
6. On the management server, paste the device ID into the list of hardware devices.

To obtain a device ID from Control Panel

1. On the Windows taskbar, click **Start > Settings > Control Panel > System**.
2. On the **Hardware** tab, click **Device Manager**.
3. In the **Device Manager** list, double-click the device.
4. In the device's **Properties** dialog box, on the **Details** tab, select the Device ID.

   By default, the Device ID is the first value displayed.
5. Press **Control+C** to copy the ID string.
6. Click **OK** or **Cancel**.

See "Adding a hardware device to the Hardware Devices list" on page 559.

Adding a hardware device to the Hardware Devices list

After you obtain a class ID or device ID for a hardware device, you can add the hardware device to the default Hardware Devices list. You can then access this default list from the device control part of the Application and Device Control Policy.

See "About hardware devices" on page 557.

To add hardware devices to the Hardware Devices list

1. In the console, click **Policies**.
2. Under Policy Components, click **Hardware Devices**.
3. Under Tasks, click **Add a Hardware Device**.
4. Enter the name of the device you want to add.

   Both Class IDs and Device IDs are enclosed in curly braces by convention.
5. Select either **Class ID** or **Device ID**, and paste the ID that you copied from the Windows Device Manager or the DevViewer tool.
6. You can use wildcard characters to define a set of device IDs. For example, you can use the following string: `*IDE\CDROM*`.

   See "Obtaining a class ID or device ID" on page 559.
7. Click **OK**.

Editing a hardware device in the Hardware Devices list

You can edit any hardware devices that you have added to the list. The default devices that are listed cannot be edited.

See "About hardware devices" on page 557.

To edit a hardware device in the Hardware Devices list

1. In the console, click **Policies**.
2. Under Policy Components, click **Hardware Devices**.
3. In the Hardware Devices list, click the hardware device you want to edit.
4. Click **Edit the Hardware Device**.
5. Edit either the device name, the class ID, or the device ID.
6. Click **OK**.

   The updated device information is displayed in the Identification list.

About authorizing the use of applications, patches, and utilities

Symantec Endpoint Protection Manager gives you the ability to protect client computers from attacks by unapproved applications. It gives you the ability in two ways. First it lets you use file fingerprints to identify approved applications, patches, and the utilities that can run on the client computers. You then decide the action to take when unapproved applications try to access the client computers. If you enable system lockdown, you can then configure Symantec Endpoint Protection Manager to either only log unapproved applications or to use system lockdown to protect those client computers that come under attack by unauthorized programs.

See "About system lockdown" on page 567.

To use system lockdown, you first create a file fingerprint list for each type of client in your environment. A file fingerprint list is a list of approved applications for that client computer. Then you add each of these file fingerprints to a file fingerprint list on the Symantec Endpoint Protection Manager. Lastly, you configure the action to take on the client when an unapproved application tries to access that computer.

For example, create a file fingerprint list for each type of client in your environment. Assume that your environment contains Windows Vista 32-bit, Windows Vista 64-bit, and Windows XP SP2 clients. Run the file, Checksum.exe, on an image of each of these three client types that exist in your environment. Checksum.exe generates file fingerprints for all of the applications for each client type and puts them into a file fingerprint list. In this example, you end up with three file fingerprint lists: one for each image.

Next, use Symantec Endpoint Protection to create a file fingerprint list to which you add each of the three file fingerprint lists you generated: one file fingerprint list for each client type. Then, you define what action Symantec Endpoint Protection takes when an unapproved application tries to access a client computer. You can disable system lockdown and allow application access. You can choose to only log the unapproved applications. For the most protection, you can enable system lockdown on the client computer that the unauthorized application is trying to access.

See "About creating and importing a file fingerprint list" on page 561.

About creating and importing a file fingerprint list

A file fingerprint list consists of a list of checksums, or file fingerprints, for each application on that client computer along with the complete file paths of those

applications. You can create a file fingerprint list from a software image that includes all the applications that you want to allow users to run on their computers.

See "About authorizing the use of applications, patches, and utilities" on page 561.

To create a file fingerprint list, you can use the utility Checksum.exe that is installed along with Symantec Endpoint Protection on the client computer. You can run this command on each computer image in your environment to create a file fingerprint list for those images.

The file Checksum.exe is located in the following location:

C:\Program Files\Symantec\Symantec Endpoint Protection

You can run this tool from the command prompt. Checksum.exe creates a text file that contains a list of all executables on that computer and their corresponding checksums.

See "Creating a file fingerprint list" on page 562.

You can use Symantec Endpoint Protection Manager to import file fingerprint lists for each client computer type into a master file fingerprint list. You can also add file fingerprints for individual files that you want to approve.

For example, you can create a file fingerprint list for each type of client in your environment. Assume that your environment contains Windows Vista 32-bit, Windows Vista 64-bit, and Windows XP SP2 clients. Run the checksum utility on an image of each of these three client types that exist in your environment. You can then import the three file fingerprint lists into Symantec Endpoint Protection Manager.

See "Importing a file fingerprint list into Symantec Endpoint Protection Manager" on page 565.

You can also merge multiple file fingerprint lists that exist in a shared policy.

See "Merging file fingerprint lists in Symantec Endpoint Protection Manager " on page 565.

You can also delete file fingerprints if you no longer use them in your configuration.

See "Deleting a file fingerprint list" on page 566.

Creating a file fingerprint list

You can use Checksum.exe to create a file fingerprint list. The file fingerprint list names each file and corresponding checksum that resides on the client computer image. This utility is provided with Symantec Endpoint Protection on the client.

See "About creating and importing a file fingerprint list" on page 561.

A sample of a Checksum.exe output file that was run on a computer image follows. The format of each line is *checksum_of_the_file* space *full_pathname_of_the_exe_or_DLL*.

```
0bb018fad1b244b6020a40d7c4eb58b7 c:\dell\openmanage\remind.exe
35162d98c2b445199fef95e838feae4b c:\dell\pnp\m\co\HSFCI008.dll
77e4ff0b73bc0aeaaf39bf0c8104231f c:\dell\pnp\m\co\HSFHWBS2.sys
f59ed5a43b988a18ef582bb07b2327a7 c:\dell\pnp\m\co\HSF_CNXT.sys
60e1604729a15ef4a3b05f298427b3b1 c:\dell\pnp\m\co\HSF_DP.sys
4f3ef8d2183f927300ac864d63dd1532 c:\dell\pnp\m\co\HXFSetup.exe
dcd15d648779f59808b50f1a9cc3698d c:\dell\pnp\m\co\MdmXSdk.dll
eeaea6514ba7c9d273b5e87c4e1aab30 c:\dell\pnp\m\co\MDMXSDK.sys
0a7782b5f8bf65d12e50f506cad6d840 c:\dell\pnp\mgmt\drac2wdm.sys
9a6d7bb226861f6e9b151d22b977750d c:\dell\pnp\mgmt\racser.sys
d97e4c330e3c940ee42f6a95aec41147 c:\dell\pnp\n\bc\b57xp32.sys
```

To create a file fingerprint list

1. Go to the computer that contains the image for which you want to create a file fingerprint list. The computer must have Symantec Endpoint Protection client software installed.
2. Open a command prompt window.
3. Navigate to the directory that contains the file Checksum.exe. By default, this file is located in the following location:

   C:\Program Files\Symantec\Symantec Endpoint Protection
4. Type the following command:

   ```
   checksum.exe outputfile drive
   ```

   where *outputfile* is the name of the text file that contains the checksums for all the executables that are located on the specified drive. The output file is a text file (*outputfile.txt)*.

   The following is an example of the syntax you use:

   ```
   checksum.exe cdrive.txt c:\
   ```

   This command creates a file that is called cdrive.txt. It contains the checksums and file paths of all the executables and DLLs found on the C drive of the client computer on which it was run.

Editing a file fingerprint list in Symantec Endpoint Protection Manager

You cannot directly edit an existing file fingerprint list. Instead, you can append an existing fingerprint list with a new list that you created from Checksum.exe. Or you can merge an existing fingerprint list with another fingerprint list that you already imported.

See "About creating and importing a file fingerprint list" on page 561.

If you want to merge fingerprint lists into a new list with a different name, use the **Add a File Fingerprint Wizard**.

See "Merging file fingerprint lists in Symantec Endpoint Protection Manager " on page 565.

To edit a file fingerprint list

1. In the console, click **Policies**.
2. Under **View Policies**, expand **Policy Components**, and then click **File Fingerprint Lists**.
3. In the **File Fingerprint Lists** pane, select the fingerprint list that you want to edit.
4. Click **Edit**.
5. In the **Edit File Fingerprint Wizard**, click **Next**.
6. Do one of the following:
   - Click **Append a fingerprint file to this file fingerprint** to add a new file to the existing one, and then click **Next**.
   - Click **Append another file fingerprint to this file fingerprint** to merge file fingerprint lists that you already imported.
7. Do one of the following:
   - In the **Import File Fingerprint** panel, click **Browse** to locate the file or type the full path of the file fingerprint list in the text box.
   - In the **Merge Multiple File Fingerprints** panel, select the file fingerprints that you want to merge.
8. Click **Next**.
9. Click **Close**.
10. Click **Finish**.

Importing a file fingerprint list into Symantec Endpoint Protection Manager

You can add file a file fingerprint list to a shared policy by importing a file. You must have created the list already.

See "About creating and importing a file fingerprint list" on page 561.

See "Creating a file fingerprint list" on page 562.

To import a file fingerprint list into a shared policy

1. In the console, click **Policies**
2. Under **View Policies**, expand **Policy Components**, and then click **File Fingerprint List**.
3. Under **Tasks**, click **Add a File Fingerprint List**.
4. In the **Welcome to the Add File Fingerprint Wizard**, click **Next**.
5. In the **Information about New File Fingerprint** panel, type a name and description for the new merged list.
6. Click **Next**.
7. In the **Create a File Fingerprint** panel, click **Create the file fingerprint by importing a file fingerprint file**.
8. Click **Next**.
9. Click **Browse** to locate the file, or type the full path of the file fingerprint list in the text box.
10. Click **Next**.
11. Click **Close**.
12. Click **Finish**.

    The new list appears under **File Fingerprint Lists**.

Merging file fingerprint lists in Symantec Endpoint Protection Manager

You can merge multiple file fingerprint lists that exist in a shared policy. You must have already added the lists that you want to merge before you start this task.

See "About creating and importing a file fingerprint list" on page 561.

See "Importing a file fingerprint list into Symantec Endpoint Protection Manager" on page 565.

To merge file fingerprint lists

1. In the console, click **Policies**.
2. Under View Policies, expand **Policy Components**, and then click **File Fingerprint Lists**.
3. Under Tasks, click **Add a File Fingerprint List**.
4. In the **Welcome to the Add File Fingerprint Wizard**, click **Next**.
5. In the **Information about New File Fingerprint** panel, type a name and description for the new merged list.
6. Click **Next**.
7. In the **Create a File Fingerprint** panel, click **Create the file fingerprint by combining multiple existing file fingerprints**.

   This option is only available if you have already imported multiple file fingerprint lists.
8. Click **Next**.
9. Select the fingerprint lists that you want to merge.
10. Click **Next**.
11. Click **Close**.
12. Click **Finish**.

    The merged fingerprint list appears under **File Fingerprint Lists**.

Deleting a file fingerprint list

You can delete any file fingerprint lists that you no longer need. First make sure that the file fingerprint list is no longer needed at the group level before you delete it from a shared policy.

See "About creating and importing a file fingerprint list" on page 561.

To delete a file fingerprint list

1. In the console, click **Policies**.
2. Under View Policies, expand **Policy Components**, and then click **File Fingerprint List**.
3. In the File Fingerprint Lists pane, click the file fingerprint list that you want to delete.

4 Under Tasks, click **Delete the List**.

5 Click **Yes** to confirm.

The file fingerprint list is deleted from the Symantec Endpoint Protection Manager, but it remains on the computer in the location from which you imported it.

About system lockdown

System lockdown is a protection setting that you can use to control the applications that can run on the client computer. You can create a file fingerprint list that contains the checksums and the locations of all the applications that are authorized for use at your company. The client software includes a Checksum.exe tool that you can use to create a file fingerprint list. The advantage of system lockdown is that it can be enforced whether or not the user is connected to the network.

You can use system lockdown to block almost any Trojan horse, spyware, or malware that tries to run or load itself into an existing application. For example, you can prevent these files from loading into Internet Explorer. System lockdown ensures that your system stays in a known and trusted state.

Applications that run on the client computer can include the following executable files:

- .exe
- .com
- .dll
- .ocx

Symantec recommends that you implement system lockdown in the following stages:

Get an approved software image	Create a software image that includes all of the applications you want users to be able to use on their computers. Use this image to create a file fingerprint list.
Log unapproved applications	Enable system lockdown by logging the applications that are not included in the file fingerprint list. You can then adjust your file fingerprint to include the required applications of users. You can give them appropriate warning before blocking unapproved applications.

Add allowed applications	Add the executables that you want to be allowed even if they are not in the file fingerprint list.
Enable system lockdown	Enforce system lockdown and block unapproved applications.

You have the option to define a custom message to display to users who have blocked applications.

See "System lockdown prerequisites" on page 568.

See "Setting up system lockdown" on page 569.

See "About authorizing the use of applications, patches, and utilities" on page 561.

System lockdown prerequisites

The following prerequisites must be met before you can enable system lockdown:

Create file fingerprint list	You need to have created a file fingerprint list that includes the applications that are allowed. This list can be created from a corporate image that is installed regularly on users' computers. You create this list on a computer that runs the client.
Add one or more file fingerprint lists	After you create the fingerprint lists, you need to add them to the manager.
Merge file fingerprint lists	Multiple file fingerprint lists can be merged. For example, you may use different images for different groups at your company.

You implement system lockdown in the following stages:

Set up and test system lockdown	Before you block unapproved executables, you can add one or more file fingerprint lists. Add the applications that should always be allowed, and log the results in the Control log.
Check the unapproved applications list	After a few days of testing system lockdown, you can view the list of unapproved applications. This list shows the unapproved applications that users in the group run. You can decide whether to add more applications to the file fingerprint or to the allowed list.

Enable system lockdown	Next, you can enable system lockdown blocking the applications that are not included in the file fingerprint lists.

See "About system lockdown" on page 567.

Setting up system lockdown

To set up system lockdown, you follow a two-step process:

- In step 1, you monitor the applications that the client computers run.
  In this step, you can track these applications in a list of unapproved applications. The list of unapproved applications includes the applications that clients run but are not listed in the file fingerprint list of approved applications. The client does not block the unapproved applications. You can track the applications that clients use for informational purposes before you block those applications. You can also test whether any applications appear on the unapproved applications list. If a test runs, the status says how long it has been running and whether or not exceptions have occurred. Run system lockdown in test mode long enough to discover which unapproved applications the client computers run. Then enable system lockdown.
  See "About system lockdown" on page 567.
  See "System lockdown prerequisites" on page 568.
- In step 2, you enable system lockdown.
  After you run system lockdown in test mode long enough to see which unapproved applications are run, you enable the following settings:

Approve the use of those additional applications	Add applications to the list of approved applications, or add the applications to the image where you created the file fingerprint.
Notify users	You can notify a user that the user no longer has access to a computer. You can also inform the user that the specified applications can be used at some future date that you state. You then proceed to enable system lockdown on that date.
Continue to log the use of the unapproved applications	No further action is necessary.

Note: You can also create firewall rules to allow approved applications on the client.

To set up system lockdown

1. On the console, click **Clients**.
2. Under View Clients, locate the group for which you want to set up system lockdown.
3. On the Policies tab, click **System Lockdown**.
4. In the System Lockdown for *name of group* dialog box, click **Step 1: Log Unapproved Applications Only** if you want to turn on this protection in test mode.

   This option logs the unapproved network applications that clients are currently running.
5. Click **Step 2: Enable System Lockdown** if you want to turn on this protection. This step blocks the unapproved applications that clients try to run.
6. Under Approved Applications, add or remove file fingerprint lists or specific files.

   See "Editing a file fingerprint list in Symantec Endpoint Protection Manager" on page 564.
7. Check **Test Before Removal** for the file fingerprint lists or applications that you want to test before you remove permanently remove them.

   When you check this option, the associated applications are logged in the Control log as unapproved applications. However, the applications are not blocked on your client computers. You can permanently remove the file fingerprint list or applications later.
8. To view the list of unapproved applications, click **View Unapproved Applications**.

   In the Unapproved Applications dialog box, review the applications. This list includes information about the time that the application was run, the computer host name, the client user name, and the executable file name.
9. Determine how you want to handle the unapproved applications.

   You can add the names of applications that you want to allow to the list of approved applications. You can add the executable to the computer image the next time that you create a file fingerprint.
10. Click **Close**.
11. To specify the executables that are always allowed even if they are not included in the file fingerprint list, under the File Name list, click **Add**.

12 In the Add File Definition dialog box, specify the full path name of the executable file (.exe or .dll).

   Names can be specified using a normal string or regular expression syntax. Names can include wildcard characters (* for any characters and ? for one character). The name can also include environment variables such as %ProgramFiles% to represent the location of your Program Files directory or %windir% for the Windows installation directory.

13 Either leave **Use wildcard matching (* and ? supported)** selected by default, or click **Use regular expression matching** if you used regular expressions in the filename instead.

14 If you want to allow the file only when it is executed on a particular drive type, click **Only match files on the following drive types**.

   Then unselect the drive types you do not want to include. By default, all drive types are selected.

15 If you want to match by device id type, check **Only match files on the following device id type**, and then click **Select**.

16 Click the device you want in the list, and then click **OK**.

17 Click **OK**.

18 To display a message on the client computer when the client blocks an application, check **Notify the user if an application is blocked**.

19 To write a custom message, click **Notification**, type the message, and click **OK**.

20 Click **OK**.

Section 6

Configuring centralized exceptions

Chapter 34

Configuring Centralized Exceptions Policies

This chapter includes the following topics:

About Centralized Exceptions Policies

Centralized Exceptions Policies contain exceptions for the following types of scans:

- Antivirus and antispyware scans
  See "Configuring a centralized exception for antivirus and antispyware scans on Windows clients" on page 579.
  See "Configuring a centralized exception for files or folders on Mac clients" on page 583.
- TruScan proactive threat scans
  See "Configuring a centralized exception for TruScan proactive threat scans" on page 584.
- Tamper Protection scans
  See "Configuring a centralized exception for Tamper Protection" on page 585.

Note: Antivirus and antispyware scans include all Auto-Protect scans, scheduled scans, on-demand scans, or user-defined scans.

Typically, exceptions are risks or processes that you want the client software to exclude from scans. If you use exceptions on client computers, you might reduce the scan time. If you reduce the scan time, you increase system performance on the client computers.

For TruScan proactive threat scans, you might also want the client software to detect a specific process that it does not detect by default. You can create an exception to force the detection. When the detection appears in the detected processes list, you can create another exception to specify an action for the detection.

See "Configuring an exception to force TruScan proactive threat scans to detect a process" on page 585.

Note: For antivirus and antispyware scans or Tamper Protection, you use centralized exceptions to specify particular items to exclude from scans. For proactive threat scans, however, you use centralized exceptions to specify actions for detected processes or to force a detection.

When you create a Centralized Exceptions Policy, the exceptions apply to all scans of that type on the client computer that uses the policy. You can include all of the exceptions in the same policy.

Unlike other policies, the Symantec Endpoint Protection Manager console does not include a default Centralized Exceptions Policy. You must create a new policy. You can create Centralized Exceptions Policies from the Policies page, or you can create Centralized Exceptions Policies from the Clients page in the management console.

You can add exceptions to a Centralized Exceptions Policy by using the logs in the management console. You must create a Centralized Exceptions Policy before you can use this method to create exceptions.

See "Creating centralized exceptions from log events" on page 587.

About working with Centralized Exceptions Policies

You create and edit Centralized Exceptions Policies similarly to how you create and modify other types of policies. You can assign, withdraw, replace, copy, export, import, or delete a Centralized Exceptions Policy.

You typically assign a policy to multiple groups in your security network. You can create a non-shared, location-specific policy if you have specific requirements for a particular location.

To work with Centralized Exceptions Policies, you must be familiar with the basics of policy configuration.

See "Using policies to manage your network security" on page 90.

About centralized exceptions for antivirus and antispyware scans

You may want to exclude a particular security risk from antivirus and antispyware scans. You might want to exclude particular files, folders, or file extensions from the scans.

Note: You can configure exceptions for Mac clients only for files or folders.

When you exclude a security risk, scans ignore the risk. You can configure the exception so that the scans log the detection. In either case, the client software does not notify users when it detects the specified security risks. When you exclude files, folders, or extensions, the scans ignore the files, folders, or extensions.

See "Configuring a centralized exception for antivirus and antispyware scans on Windows clients" on page 579.

Note: Centralized exceptions apply to all antivirus and antispyware scans. You cannot create different exceptions for different types of scans. For example, you may want to create a centralized exception to exclude a particular file extension. The client software then excludes the extension from Auto-Protect scans and all administrator-defined scans and user-defined scans. Administrator-defined scans and user-defined scans include scheduled scans and on-demand scans.

About centralized exceptions for TruScan proactive threat scans

You may want to exclude certain processes from proactive threat scans. You need to determine that the processes that you want to exclude are safe to run on the client computers in your security network. To exclude a detected process, you set the detection action to Ignore.

You can also create a centralized exception to specify that certain processes are not permitted. To specify that processes are not permitted, you set the detection action to Quarantine or Terminate.

See "Adding a centralized exception for TruScan proactive threat scan events" on page 588.

You can force a proactive threat detection by creating a centralized exception that specifies a file name. When the proactive threat scan detects the file, the

client logs the instance. Because file names are not unique, multiple processes might use the same file name. You can use a forced detection to help you create an exception to quarantine or terminate a process that is associated with the file.

See "How TruScan proactive threat scans work with centralized exceptions" on page 526.

About centralized exceptions for Tamper Protection

Tamper Protection protects client computers from the processes that tamper with Symantec processes and internal objects. When Tamper Protection detects a process that might modify the Symantec configuration settings or Windows registry values, it blocks the process. You might need to allow an application to modify Symantec settings. You might want to stop Tamper Protection for certain areas of the registry or certain files on the client computer.

In some cases, Tamper Protection might block a screen reader or some other assistive technology application. You can create a centralized exception so that the application can run on client computers.

See "Adding a centralized exception for Tamper Protection events" on page 588.

About client interaction with centralized exceptions

Administrator-defined exceptions always take precedence over user-defined exceptions. On client computers, users cannot view the list of administrator-defined exceptions. A user can only view any exception that the user creates.

By default, users on client computers have limited configuration rights for centralized exceptions.

By default, users have the following restrictions:

- Users cannot create exceptions to force detections for proactive threat scans. Users cannot select from a list of detected processes to create an exception for proactive threat scans. However, users can select a file on the client computer to create a proactive threat scan exception.
- Users cannot create any exceptions for Tamper Protection.

You can restrict users on client computers so that they cannot create exceptions for antivirus and antispyware scans or for proactive threat scans.

See "Configuring client restrictions for centralized exceptions" on page 586.

Configuring a Centralized Exceptions Policy

You configure a Centralized Exceptions Policy in the same way that you configure other types of policies.

You can click Help for more information about the options that are used in the procedures.

To configure a Centralized Exceptions Policy

1. On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
2. Under **Centralized Exceptions**, click **Add**, and then perform any of the following actions:
   - Click **Windows Exceptions > Security Risk Exceptions**, or **Mac Exceptions > Security Risk Exception for File or Folder**. Then, add the security risk exceptions that you want to include in the policy.
     See "Configuring a centralized exception for antivirus and antispyware scans on Windows clients" on page 579.
     See "Configuring a centralized exception for files or folders on Mac clients" on page 583.
   - Click **Windows Exceptions > TruScan Proactive Threat Scan Exceptions**, and then add a proactive threat scan exception that you want to include in the policy.
     See "Configuring a centralized exception for TruScan proactive threat scans" on page 584.
   - Click **Windows Exceptions > Tamper Protection Exception**, and then add a Tamper Protection scan exception that you want to include in the policy.
     See "Configuring a centralized exception for Tamper Protection" on page 585.
3. Repeat step 2 to add more exceptions.
4. If you are finished with the configuration for this policy, click **OK**.

Configuring a centralized exception for antivirus and antispyware scans on Windows clients

You can create exceptions for known security risks, files, folders, or file extensions. The exceptions apply to all antivirus and antispyware scans that run on the client computers that use the policy.

Note: You can create an exception only for files or folders for Mac clients.

See "Configuring a centralized exception for files or folders on Mac clients" on page 583.

You can click Help for more information about the options that are used in the procedure.

To configure a centralized exception for antivirus and antispyware scans on Windows clients

1. On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
2. Under **Centralized Exceptions**, click **Add > Windows Exceptions > Security Risk Exceptions**, and then perform one of the following actions:
   - Click **Known Risks**, and then configure the exception.
     See "Configuring centralized exceptions for known security risks" on page 580.
   - Click **File**, and then configure the exception.
     See "Configuring a centralized exception for a file for Windows clients" on page 581.
   - Click **Folder**, and then configure the exception.
     See "Configuring a centralized exception for a folder for Windows clients" on page 582.
   - Click **Extensions**, and then configure the exception.
     See "Configuring a centralized exception for a file extension" on page 582.
3. Click **OK**.
4. If you are finished with the configuration for this policy, click **OK**.

Configuring centralized exceptions for known security risks

The security risks that the client software detects appear in the Known Security Risk Exceptions dialog box.

See "Configuring a centralized exception for antivirus and antispyware scans on Windows clients" on page 579.

The known security risks list includes information about the severity of the risk.

You can click Help for more information about the centralized exceptions options for known security risks.

To configure centralized exceptions for known security risks

1. On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
2. Under Centralized Exceptions, click **Add > Windows Exceptions > Security Risk Exceptions > Known Risks**.
3. In the Known Security Risk Exceptions dialog box, select one or more security risks that you want to exclude from antivirus and antispyware scans.
4. Check **Log when the security risk is detected** if you want to log the detection.

   If you do not check this option, the client ignores the risk when it detects the selected risks. The client therefore does not log the detection.
5. Click **OK**.
6. If you are finished with the configuration for this policy, click **OK**.

Configuring a centralized exception for a file for Windows clients

You add exceptions for files individually. If you want to create exceptions for more than one file, repeat the procedure.

See "Configuring a centralized exception for antivirus and antispyware scans on Windows clients" on page 579.

To configure a centralized exception for a file for Windows clients

1. On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
2. Under **Centralized Exceptions**, click **Add > Windows Exceptions > Security Risk Exceptions > File**.
3. Under **Security Risk File Exception**, in the **Prefix variable** drop-down box, select a common folder.

   When you select a prefix, the exception can be used on different Windows operating systems.

   Select **[NONE]** if you want to enter the absolute path and file name.

   Note: Folder paths for Windows clients must be denoted by using a backward slash.
4. In the **File** text box, type the name of the file.

   If you selected a prefix variable, the path should be relative to the prefix. If you selected **[NONE]**, type the full path name of the file.

5 Click **OK**.

6 If you are finished with the configuration for this policy, click **OK**.

Configuring a centralized exception for a folder for Windows clients

You add exceptions for folders individually. If you want to create exceptions for more than one folder, repeat the procedure.

See "Configuring a centralized exception for antivirus and antispyware scans on Windows clients" on page 579.

To configure a centralized exception for a folder for Windows clients

1 On the Centralized Exceptions Policy page, click **Centralized Exceptions**.

2 Under **Centralized Exceptions**, click **Add > Windows Exceptions > Security Risk Exceptions > Folder**.

3 Under **Security Risk Folder Exception**, in the **Prefix variable** drop-down box, select a common folder.

When you select a prefix, the exception can be used on different Windows operating systems.

Select **[NONE]** if you want to enter the absolute path and file name.

Note: Folder paths for Windows clients must be denoted by using a backward slash.

---

4 In the **Folder** text box, type the name of the folder.

If you selected a prefix variable, the path should be relative to the prefix. If you selected **[NONE]**, type the full path name.

5 Click **OK**.

6 If you are finished with the configuration for this policy, click **OK**.

Configuring a centralized exception for a file extension

You can add multiple file extensions to an exception. After you create the exception, you cannot create another extensions exception for the same policy. You must edit the existing exception.

See "Configuring a centralized exception for antivirus and antispyware scans on Windows clients" on page 579.

Note: You can add only one extension at a time. If you enter multiple extension names in the Add text box, the policy treats the entry as a single extension name.

To configure a centralized exception for a file extension

1. On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
2. Under Centralized Exceptions, click **Add > Windows Exceptions > Security Risk Exceptions > Extension**.
3. In the text box, type the extension that you want to exclude, and then click **Add**.
4. Repeat step 3 to add more extensions to the exception.
5. Click **OK**.
6. If you are finished with the configuration for this policy, click **OK**.

Configuring a centralized exception for files or folders on Mac clients

If you configure a centralized exception for files or folders on Mac clients, you must select the appropriate option in the Antivirus and Antispyware policy for Auto-Protect scans.

See "Configuring File System Auto-Protect for Mac clients" on page 435.

See "Configuring a Centralized Exceptions Policy" on page 579.

To configure a centralized exception for files or folders on Mac clients

1. On the Centralized Exceptions policy page, click **Centralized Exceptions**.
2. Under **Centralized Exceptions**, click **Add > Mac Exceptions > Security Risk Exceptions for File or Folder**.
3. Under **Security Risk File or Folder Exception**, in the **Prefix variable** drop-down box, select a common folder.

   Select **[NONE]** to enter the absolute path and file name.

   Note: Folder paths for Mac clients must be denoted by using a forward slash.

4. In the **Folder** text box, type the name of the folder.

   If you select a prefix variable, the path should be relative to the prefix. If you select **[NONE]**, type the full path name.
5. Click **OK**.
6. If you are finished with the configuration for this policy, click **OK**.

Configuring a centralized exception for TruScan proactive threat scans

You can configure exceptions to exclude detected processes from future proactive threat scans. You can also force a proactive threat scan to detect a particular process.

To configure a centralized exception for TruScan proactive threat scans

1. On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
2. Click **Add > Windows Exceptions > TruScan Proactive Threat Scan Exceptions**, and then do one of the following actions:
   - Click **Detected Processes**.
     See "Configuring a centralized exception for a detected process" on page 584.
   - Click **Process**.
     See "Configuring an exception to force TruScan proactive threat scans to detect a process" on page 585.
3. Click **OK**.
4. If you are finished with the configuration for this policy, click **OK**.

Configuring a centralized exception for a detected process

You can create an exception for a process that TruScan proactive threat scans detect.

When you create an exception for a detected process, you choose from a list of detections. The management console populates the list with the detections that the client logs in your security network.

The detection list appears empty if the client computers in your network have not yet made any detections.

You can force proactive threat scans to detect a particular process. When a proactive threat scan detects the process, and the management console receives the event, the process appears in the detected process list.

See "Configuring an exception to force TruScan proactive threat scans to detect a process" on page 585.

To configure a centralized exception for a detected process

1. On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
2. Click **Add > Windows Exceptions > TruScan Proactive Threat Scan Exceptions > Detected Processes**.
3. Select the processes for which you want to create an exception.

4 In the Action drop-down box, select **Ignore**, **Terminate**, **Quarantine**, or **Log only**.

5 Click **OK**.

6 If you are finished with the configuration for this policy, click **OK**.

Configuring an exception to force TruScan proactive threat scans to detect a process

You can configure an exception to force proactive threat scans to detect a process. You might configure this type of exception when proactive threat scans currently do not detect a particular process.

After future scans run and detect the specified process, you can create another exception to handle the process.

See "Configuring a centralized exception for a detected process" on page 584.

To configure an exception to force TruScan proactive threat scans to detect a process

1 On the Centralized Exceptions Policy page, click **Centralized Exceptions**.

2 Click **Add > Windows Exceptions > TruScan Proactive Threat Scan Exceptions > Process**.

3 In the dialog box, type the process name.

For example, you might type the name of an executable file as follows:

foo.exe

4 Click **OK**.

5 If you are finished with the configuration for this policy, click **OK**.

Configuring a centralized exception for Tamper Protection

You can configure centralized exceptions for Tamper Protection. You need to know the file name that is associated with the application that you want to allow.

For example, Tamper Protection might block an assistive technology application, such as a screen reader. You need to know the name of the file that is associated with the assistive technology application. Then you can create an exception to allow the application to run.

See "Configuring a Centralized Exceptions Policy" on page 579.

To configure a centralized exception for Tamper Protection

1. On the Centralized Exceptions Policy page, click **Centralized Exceptions**.
2. Click **Add > Windows Exceptions > Tamper Protection Exception**.
3. In the **Add Tamper Protection Exception** dialog box, in the **Prefix variable** drop-down box, select a common folder.

   When you select a prefix, the exception can be used on different Windows operating systems.

   Select **[NONE]** if you want to enter the absolute path and file name.
4. In the **File** text box, type the name of the file.

   If you selected a prefix, the path should be relative to the prefix. If you selected **[NONE]** for the prefix, type the full path name.
5. Click **OK**.
6. If you are finished with the configuration for this policy, click **OK**.

Configuring client restrictions for centralized exceptions

You can configure restrictions so that users on client computers cannot create exceptions for antivirus and antispyware scans or for TruScan proactive threat scans. By default, users are permitted to configure exceptions. For proactive threat scans, users have limited configuration privileges.

See "About client interaction with centralized exceptions" on page 578.

You can click Help for more information about the options that are used in the procedure.

Note: Users on client computers can never create exceptions for Tamper Protection, regardless of the restriction settings.

To configure client restrictions for centralized exceptions

1. On the Centralized Exceptions Policy page, click **Client Restrictions**.
2. Under Client Restrictions, check or uncheck **Security risk exceptions** and **TruScan proactive threat scan exceptions**.
3. If you are finished with the configuration for this policy, click **OK**.

Creating centralized exceptions from log events

You can create centralized exceptions from log events for antivirus and antispyware scans or proactive threat scans.

When you create exceptions from log events, you add a risk, file, folder, extension, or process to the Centralized Exceptions Policy. You specify the Centralized Exceptions Policy when you create the exception.

See "About logs" on page 261.

To create centralized exceptions from log events

1. On the Monitors tab, click the **Logs** tab.
2. In the Log type drop-down list, select one of the following options:
   - **Risk**
   - **TruScan Proactive Threat Scan**
   - **Application and Device Control**
3. If you selected Application and Device Control, select **Application Control** from the Log content list.
4. Click **View Log**.
5. Follow the instructions for adding centralized exceptions for the type of log that you selected.

   See "Adding a centralized exception for risk events" on page 587.

   See "Adding a centralized exception for TruScan proactive threat scan events" on page 588.

   See "Adding a centralized exception for Tamper Protection events" on page 588.

Adding a centralized exception for risk events

You can add a centralized exception for risk events.

See "Creating centralized exceptions from log events" on page 587.

To add a centralized exception for risk events

1. On the Risk Logs page, select one or more events for which you want to add a centralized exception.
2. Next to Action, select one of the following options:
   - **Add Risk to Centralized Exceptions Policy**
   - **Add File to Centralized Exceptions Policy**

- **Add Folder to Centralized Exceptions Policy**
- **Add Extension to Centralized Exceptions Policy**

3 Click **Start**.

4 In the dialog box, you can remove any of the risks, files, folders, or extensions that are associated with the event. If you remove items, you do not include them in the exception.

If no items appear in the risks, files, folders, or extensions list, you cannot create an exception.

5 For security risks, check **Log when the security risk is detected** if you want the client software to log the detection.

6 Select all of the centralized exceptions policies that should use this exception.

7 Click **OK**.

Adding a centralized exception for TruScan proactive threat scan events

You can add a centralized exception for proactive threat scan events.

See "Creating centralized exceptions from log events" on page 587.

To add a centralized exception for TruScan proactive threat scan events

1 On the TruScan Proactive Threat Scan Logs page, select one or more events for which you want to add a centralized exception.

2 Next to Action, select **Add Process to Centralized Exceptions Policy**.

3 Click **Start**.

4 In the dialog box, in the Response drop-down list, select the detection action for the process.

Optionally, you can remove any processes that you do not want to include in the exception.

5 Select the Centralized Exceptions Policies that should include this exception.

6 Click **OK**.

Adding a centralized exception for Tamper Protection events

You can add a centralized exception for Tamper Protection events. The Tamper Protection feature must have already blocked the application that you want to allow. After Tamper Protection blocks the application, the client computer logs the event and sends it to the management server. You can use the log event to create the exception.

See "Creating centralized exceptions from log events" on page 587.

To add a centralized exception for Tamper Protection events

1. On the Application and Device Control Logs page, select one or more events for which you want to add a centralized exception.

   For example, you might select one or more events that apply to the assistive technology applications that you want to run.

2. Next to Action, select **Add File to Centralized Exceptions Policy**.
3. Click **Start**.
4. To remove a file that you do not want to include in the exception, select the file and click **Remove**.

   Repeat this step to remove more files.

5. Select the Centralized Exceptions Policies that should include this exception.
6. Click **OK**.

Appendix A

Using the command-line interface

This appendix includes the following topics:

Windows commands for the client service

You can manipulate the client directly from the command line on a Windows client computer by using the smc command for the client service. You may want to use this command in a script that runs the parameters remotely. For example, if you need to stop the client to install an application on multiple clients, you can stop and restart each client service.

The client service must run for you to use the command-line parameters, with the exception of `smc -start` parameter. The command-line parameters are not case sensitive.

Table A-1 describes the parameters that you can run if users are members of any Windows user group.

Table A-1 Parameters that all Windows members can use

Parameter	Description
smc -checkinstallation	Checks whether the `smc` client service is installed. Returns 0, -3
smc -checkrunning	Checks whether the `smc` client service is running. Returns 0, -4

Table A-1 Parameters that all Windows members can use *(continued)*

Parameter	Description
smc -dismissgui	Closes either the Symantec Endpoint Protection or Symantec Network Access Control client user interface, including the notification area icon. The client still runs and protects the client computer. Returns 0

smc -exportlog	Exports the entire contents of a log to a `.txt` file.
	To export a log, you use the following syntax:
	`smc -exportlog log_type 0 -1 output_file`
	where:
	`log_type` is:
	■ 0 = System Log
	■ 1 = Security Log
	■ 2 = Traffic Log
	■ 3 = Packet Log
	■ 4 = Control Log
	For example, you might type the following syntax:
	`smc -exportlog 2 0 -1 c:\temp\TrafficLog`
	Where:
	`0` is the beginning of the file
	`-1` is the end of the file
	You can export only the Control log, Packet log, Security log, System log, and Traffic log.
	`output_file` is the path name and file name that you assign to the exported file.
	Returns 0, -2, -5

smc -runhi	If Symantec Network Access Control is installed, runs a Host Integrity check. Returns 0
smc -showgui	Displays either the Symantec Endpoint Protection or the Symantec Network Access Control client user interface. Returns 0

Table A-1 Parameters that all Windows members can use *(continued)*

Parameter	Description
smc -updateconfig	Checks whether the configuration file on the management server is more recent than the configuration file on the client. The configuration file includes all the settings on the management server, such as policies, groups, log settings, security settings, and user interface settings. If the client's configuration file is out of date, updateconfig downloads the most recent configuration file and replaces the existing configuration file, which is serdef.dat. Returns 0

You can run the parameters in Table A-2 only if the following conditions are met:

- The client runs Windows 2003/XP/Vista, or Windows Server 2008 and users are members of the Windows Administrators group.
- The client runs Windows 2003/XP and users are members of the Power Users group.

If the client runs Windows Vista and the User Account Control is enabled, the user automatically becomes a member of both the Administrators and Users group. To use the following parameters, the user must be a member of the Administrators group only.

Table A-2 Parameters that members of the Administrators group can use

Parameter	Description
smc -exportconfig	Exports the client's configuration file to an .xml file. The configuration file includes all the settings on the management server, such as policies, groups, log settings, security settings, and user interface settings. You must specify the path name and file name. For example, you can type the following command: `smc -exportconfig C:\My Documents\MyCompanyprofile.xml` Returns 0, -1, -5, -6

Table A-2 Parameters that members of the Administrators group can use *(continued)*

Parameter	Description
smc -importconfig	Replaces the contents of the client's current configuration file with an imported configuration file. The client must run to import the configuration file's contents. You must specify the path name and file name. For example, you can type the following command: `smc -importconfig C:\My Documents\MyCompanyprofile.xml.` Returns 0, -1, -5, -6
smc -exportadvrule	Exports the client's firewall rules to a .sar file. The exported rules can only be imported into an unmanaged client or a managed client in client control mode or mixed mode. The managed client ignores these rules in server control mode. You must specify the path name and file name. For example, you can type the following command: `smc -exportadvrule C:\myrules.sar` Returns 0, -1, -5, -6
smc -importadvrule	Adds the imported firewall rules to the client's list of existing firewall rules. These rules do not overwrite the existing rules. The client lists both existing rules and imported rules, even if each rule has the same name and parameters. You can import only firewall rules into an unmanaged client or a managed client in client control mode or mixed mode. The managed client ignores these rules in server control mode. To import firewall rules, you import a .sar file. For example, you can type the following command: `smc -importadvrule C:\myrules.sar` An entry is added to the System log after you import the rules. Returns 0, -1, -5, -6
smc -start	Starts the Symantec Endpoint Protection or Symantec Network Access Control client service. Returns 0, -1

Table A-2 Parameters that members of the Administrators group can use *(continued)*

Parameter	Description
smc -stop	Stops the Symantec Endpoint Protection or Symantec Network Access Control client service and unloads it from memory. Returns 0, -1

When you import configuration files and firewall rules, note that the following rules apply:

- You cannot import configuration files or firewall rule files directly from a mapped network drive.
- The client does not support UNC (universal naming convention) paths.

Error codes

Table A-3 displays the error codes that the `smc` command returns when the required parameters are invalid or missing.

Table A-3 Smc error codes

Error code	Description
0	Command was successful.
-1	User is not in the Windows Administrators or Windows Power Users group. If the client runs Windows Vista, the user is not a member of the Windows Administrators group.
-2	Invalid parameter. You may have typed the parameter incorrectly, or you may have added an incorrect switch after the parameter.
-3	`smc` client service is not installed.
-4	`smc` client service is not running.
-5	Invalid input file. For example, the `importconfig`, `exportconfig`, `updateconfig`, `importadv`, `exportadvrule`, and `exportlog` parameters require the correct path name and file name.

Table A-3 Smc error codes *(continued)*

Error code	Description
-6	Input file does not exist. For example, the `importconfig`, `updateconfig`, and `importadvrule` parameters require the correct path name, configuration file name (.xml) or firewall rules file name (.sar).

Typing a parameter if the client is password-protected

You can set up password-protection on the client if you or another user either stops the client service or imports or exports the configuration file. You must type the password if the client is password-protected for the following parameters:

-stop	The client asks for a password before you or the user stops the client.
-importconfig	The client asks for a password before you can import the configuration file.
-exportconfig	The client asks for a password before you can export the configuration file.

See "Password-protecting the client" on page 170.

Note: The password is limited to 15 characters or less.

To type a parameter if the client is password-protected

1. On the client computer, on the taskbar, click **Start > Run**.
2. In the Run dialog box, type **cmd**

3 In the Windows MS-DOS prompt, type either one of the following parameters:

`smc -parameter -p password`

`smc -p password -parameter`

Where:

parameter is `-stop`, `-importconfig`, or `-exportconfig`.

password is the password you specified in the console.

For example, you can type either of the following syntax:

`smc -exportconfig c:\profile.xml -p password` or

`smc -p password -exportconfig c:\profile.xml`

4 Close the command prompt.

Appendix B

About client and server communication settings

This appendix includes the following topics:

About client and server communication settings

The communication settings between the client and server and other client settings are stored in files on the client computer.

Table B-1 Client files

File name	Description
SerDef.dat	An encrypted file that stores communication settings by location. Each time the user changes locations, the SerDef.dat file is read and the appropriate communication settings for the new location are applied to the client.
sylink.xml	Stores the global communication settings. This file is for internal use only and should not be edited. It contains settings from the Symantec Endpoint Protection Manager. If you edit this file, most settings will be overwritten by the settings from the management server the next time the client connects to the management server.
SerState.dat	An encrypted file that stores information about the user interface, such as the client's screen size, whether the client's console for Network Threat Protection appears, and whether Windows services appear. When the client starts, it reads this file and returns to the same user interface state as before it was stopped.

Appendix C

Client protection and management details by platform

This appendix includes the following topics:

Management features by platform

The following table explains the management options that are available for the Windows and Mac client platforms.

Table C-1 Installing, managing, and updating Symantec Endpoint Protection (Windows and Mac only)

Feature	Windows	Mac
Deploy client remotely from Symantec Endpoint Protection Manager	Yes	No
Manage client from Symantec Endpoint Protection Manager	Yes	Yes

Table C-1 Installing, managing, and updating Symantec Endpoint Protection (Windows and Mac only) *(continued)*

Feature	Windows	Mac
Update virus definitions and product from management server	Yes	No
Run commands from management server	■ Scan ■ Update Content ■ Update Content and Scan ■ Restart Client Computers ■ Enable Auto-Protect ■ Restart Client Computers ■ Enable Auto-Protect ■ Enable Network Threat Protection ■ Disable Network Threat Protection	■ Scan ■ Update Content ■ Update Content and Scan ■ Restart Client Computers ■ Enable Auto-Protect ■ Restart Client Computers ■ Enable Auto-Protect
Provide updates by using Group Update Providers	Yes	No
Run Intelligent Updater	Yes	Yes
Package updates for third-party tools in management server	Yes	No*
Set randomized scans	Yes	No
Set randomized updates	Yes	Yes

*You can, however, run Intelligent Updater to get Mac content updates. You can then push the updates to Mac clients by using a third-party tool such as Apple Remote Desktop.

See "Using the Intelligent Updater to download antivirus content updates for distribution" on page 155.

See "Using the Intelligent Updater to download antivirus content updates for distribution" on page 155.

See "Antivirus and Antispyware policy settings available for Windows and Mac" on page 604.

See "LiveUpdate policy settings available for Windows and Mac" on page 605.

See "Client protection features by platform" on page 603.

Client protection features by platform

The following table explains the differences in the protection features that are available on the different client platforms.

Table C-2 Symantec Endpoint Protection client protection

Client Feature	Windows 2000 Professional Edition, Windows XP, Windows Vista, Windows 7, 32-bit	Windows XP, Windows Vista, Windows 7, 64-bit	Windows Server 2003, Windows Server 2008, 32-bit	Windows Server 2003, Windows Server 2008, 64-bit	Mac	Linux
Scheduled scans	Yes	Yes	Yes	Yes	Yes	Yes
On-demand scans	Yes	Yes	Yes	Yes	Yes	Yes
File System Auto-Protect	Yes	Yes	Yes	Yes	Yes	Yes
Internet Email Auto-Protect	Yes	No	No	No	No	No
Microsoft Outlook Auto-Protect	Yes	No	Yes	No	No	No
Lotus Notes Auto-Protect	Yes	No	Yes	No	No	No
TruScan Proactive Threat Scans	Yes	Yes	Yes	Yes	No	No
Firewall	Yes	Yes	Yes	Yes	No	No
Intrusion Prevention	Yes	Yes	Yes	Yes	No	No
Application and Device Control	Yes	No	Yes	No	No	No
Host Integrity	Yes	Yes	Yes	Yes	No	No
Tamper Protection	Yes	No	Yes	No	No	No

See "Management features by platform" on page 601.

See "Antivirus and Antispyware policy settings available for Windows and Mac" on page 604.

See "LiveUpdate policy settings available for Windows and Mac" on page 605.

Antivirus and Antispyware policy settings available for Windows and Mac

Table C-3 displays the differences in the policy settings that are available for Windows clients and Mac clients.

Table C-3 Antivirus and Antispyware policy settings (Windows and Mac only)

Policy setting	Windows	Mac
Define actions for scans	You can specify first and second actions when different types of virus or risk are found. You can specify the following actions: ■ Clean ■ Quarantine ■ Delete ■ Leave alone	You can specify either of the following actions: ■ Automatically repair infected files ■ Quarantine files that cannot be repaired
Specify remediation if a virus or a risk is found	You can specify the following remediation actions: ■ Back up files before repair ■ Terminate processes ■ Stop services	Remediation is automatically associated with actions.
Set scan type	Active, Full, Custom	Custom only
Retry scheduled scans	Yes	No
Set scans to check additional locations (scan enhancement)	Yes	No
Configure storage migration scans	Yes	No
Configure scan exceptions	Configure Centralized Exceptions policy only	Specify setting in Antivirus and antispyware policy and configure Centralized Exceptions policy

See "Management features by platform" on page 601.

See "LiveUpdate policy settings available for Windows and Mac" on page 605.

See "Client protection features by platform" on page 603.

LiveUpdate policy settings available for Windows and Mac

Table C-4 displays the LiveUpdate Settings policy options that the Windows client and Mac clients support.

Table C-4 LiveUpdate policy settings (Windows and Mac only)

Policy setting	Windows	Mac
User the default management server	Yes	No
Use a LiveUpdate server (internal or external)	Yes	Yes
Use a Group Update Provider	Yes	No
Enable third party content management	Yes	No*
LiveUpdate Scheduling	Yes	Yes
User Settings	Yes	No
Product Update Settings	Yes	Yes

*You can, however, run Intelligent Updater to get Mac content updates. You can then push the updates to Mac clients by using a third-party tool such as Apple Remote Desktop.

See "Using the Intelligent Updater to download antivirus content updates for distribution" on page 155.

See "Management features by platform" on page 601.

See "Antivirus and Antispyware policy settings available for Windows and Mac" on page 604.

See "Client protection features by platform" on page 603.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z