

# Symantec™ Endpoint Protection Evaluation Guide



# Symantec™ Endpoint Protection Evaluation Guide

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

Documentation version 11.00.02.00.00

## Legal Notice

Copyright © 2008 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, LiveUpdate, Sygate, Symantec AntiVirus, Bloodhound, Confidence Online, Digital Immune System, Norton, and TruScan are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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

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

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

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

Symantec Corporation  
20330 Stevens Creek Blvd.  
Cupertino, CA 95014

<http://www.symantec.com>

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

# Technical Support

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

Symantec's maintenance offerings include the following:

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

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

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

## Contacting Technical Support

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

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

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

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

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

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

## Licensing and registration

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

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/techsupp/](http://www.symantec.com/techsupp/)

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

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

## Maintenance agreement resources

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

Asia-Pacific and Japan	<a href="mailto:contractsadmin@symantec.com">contractsadmin@symantec.com</a>
Europe, Middle-East, and Africa	<a href="mailto:semea@symantec.com">semea@symantec.com</a>
North America and Latin America	<a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a>

## Additional enterprise services

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

Enterprise services that are available include the following:

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

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

[www.symantec.com](http://www.symantec.com)

Select your country or language from the site index.

# Contents

Technical Support .....	4
Chapter 1	Introducing Symantec Endpoint Protection ..... 11
	Introduction to Symantec Endpoint Protection ..... 11
	About Symantec Endpoint Protection ..... 12
	About Network Threat Protection ..... 13
	About Proactive Threat Protection ..... 14
	About Antivirus and Antispyware Threat Protection ..... 14
	About Symantec ..... 15
Chapter 2	Installing Symantec Endpoint Protection ..... 17
	System installation requirements ..... 17
	Symantec Endpoint Protection Manager, Console, and database ..... 17
	Symantec Endpoint Protection Manager and Console ..... 19
	Symantec Endpoint Protection Console ..... 20
	Symantec Endpoint Protection ..... 22
	Installation process overview ..... 23
	About Desktop firewalls and communications ports ..... 24
	Installing and configuring Symantec Endpoint Protection Manager ..... 27
	Installing Symantec Endpoint Protection Manager with an embedded database ..... 30
	Installing Symantec Endpoint Protection Manager with a Microsoft SQL database ..... 30
	Logging on to the Symantec Endpoint Protection Manager Console ..... 42
Chapter 3	Configuring your product after installation ..... 43
	Setting up the organizational structure and updating content ..... 43
	Adding a group ..... 44
	About importing the organizational structure ..... 45
	Adding clients as users or as computers ..... 45
	Adding a location with a wizard ..... 46

Adding an administrator account ..... 48  
About LiveUpdate Policies ..... 49  
Configuring a LiveUpdate Settings Policy ..... 50  
Configuring a LiveUpdate Content Policy ..... 51

## Chapter 4

Creating policies ..... 53  
About policies ..... 53  
Evaluating policies ..... 55  
    Adding a shared policy ..... 56  
    Assigning a shared policy ..... 57  
    Updating the policy file manually ..... 58  
    Verifying that policies have been updated ..... 58  
Setting up and testing an Antivirus and Antispyware Policy ..... 59  
    About Antivirus and Antispyware Policies ..... 60  
    About the preconfigured Antivirus and Antispyware Policies ..... 61  
    Adding scheduled scans to an Antivirus and Antispyware  
    Policy ..... 62  
    Configuring actions for known virus and security risk  
    detections ..... 63  
    About notification messages on infected computers ..... 64  
    Customizing and displaying notifications on infected  
    computers ..... 65  
    Testing to see that the Antivirus and Antispyware Policy  
    works ..... 67  
    About TruScan proactive threat scans ..... 67  
    About using the Symantec default settings ..... 68  
    About the processes that TruScan proactive threat scans  
    detect ..... 69  
    About managing false positives detected by TruScan proactive  
    threat scans ..... 70  
    About the processes that TruScan proactive threat scans  
    ignore ..... 72  
    Understanding TruScan proactive threat detections ..... 73  
Setting up and testing a Firewall Policy ..... 76  
    About firewall rules ..... 77  
    Creating a Firewall Policy to allow or block an application ..... 78  
    Testing the Firewall Policy ..... 79  
Setting up and testing a custom IPS library ..... 80  
    About custom IPS signatures ..... 80  
    About creating custom IPS signatures to detect an attempt to  
    download MP3 files ..... 82  
    Creating custom IPS signatures ..... 84

	Testing the custom IPS signature .....	88
	Setting up and testing an Application and Device Control Policy .....	89
	Enabling a default application control rule set .....	90
	Creating a new application control rule set and adding a new rule to the set .....	91
	About device control .....	99
	About hardware devices .....	100
	Obtaining a class ID or device ID .....	101
	Adding a hardware device to the Hardware Devices list .....	101
	Configuring device control for an Application and Device Control Policy .....	102
Chapter 5	Creating client installation packages .....	105
	Creating client installation packages .....	105
	About client installation packages .....	106
	Configuring installation package features .....	106
	Configuring client installation package settings .....	107
	Exporting client installation packages .....	107
	Deploying client software with the Push Deployment Wizard .....	109
Chapter 6	Configuring Host Integrity for endpoint compliance .....	111
	Setting up and testing a Host Integrity Policy .....	111
	Adding Host Integrity requirements .....	113
	Adding a predefined firewall requirement .....	115
	Adding a custom requirement that checks whether the client computer runs an antivirus software package .....	116
	Testing to see if the Host Integrity Policy works .....	117
	Running a Host Integrity check .....	118
	Viewing the Network Access Control logs .....	118
	Configuring peer-to-peer authentication .....	119
Chapter 7	Using logs and reports to monitor security .....	121
	About logs and reports .....	121
	About the Symantec Endpoint Protection Home page .....	122
	About logs .....	127
	About log types, contents, and commands .....	128
	Viewing logs .....	133
	Displaying event details in logs .....	135
	Viewing logs from other sites .....	135
	Running commands and actions from logs .....	136

Using notifications .....	139
Viewing and filtering administrator notification information .....	139
Threshold guidelines for administrator notifications .....	140
Creating administrator notifications .....	141
About editing existing notifications .....	145
Creating quick reports .....	145

# Introducing Symantec Endpoint Protection

This chapter includes the following topics:

- [Introduction to Symantec Endpoint Protection](#)
- [About Symantec Endpoint Protection](#)
- [About Symantec](#)

## Introduction to Symantec Endpoint Protection

Symantec Endpoint Protection provides a single, integrated security solution that protects against the sophisticated attacks that evade traditional security measures. Symantec Endpoint Protection proactively secures endpoints against known and unknown threats by combining antivirus technology with advanced threat prevention.

In a single unit, managed from a single management console, it contains the following essential security technologies:

- Antivirus and antispymware
- Desktop firewall
- Intrusion prevention system (IPS)
- Application control and device control

It offers proven world-class protection in a single package to reduce overhead, time, and costs. Companies can efficiently manage security and gain the confidence that their assets and business are protected.

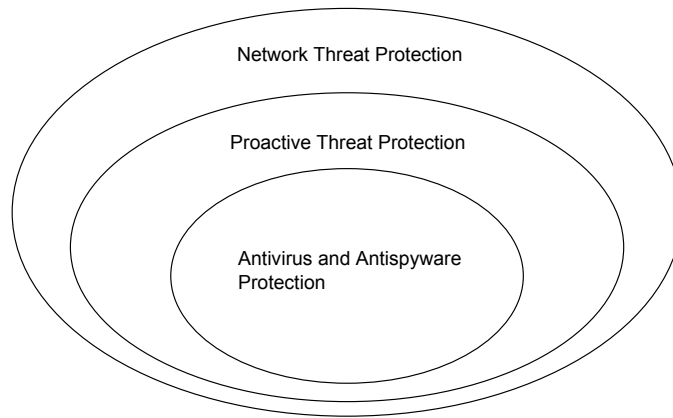
Symantec Endpoint Protection offers the following benefits:

- Provides better protection at the client level.  
Multiple integrated security technologies provide better protection for all clients in a corporate network that includes remote users and laptops, with multiple integrated security technologies.
- Simplifies the management.  
Multiple security components are managed centrally. Central management provides administrators with a comprehensive security view for the client and simplifies overall security management. An integrated solution with centralized management and response allows customers to see a more comprehensive view of the client level. This solution responds quickly to outbreaks by retrieving and deploying integrated updates from a centralized management console.
- Enables a quicker response time.  
Central management of integrated antivirus and antispyware, firewall, and intrusion prevention gives administrators the ability to respond quickly against multiple types of security threats.
- Reduces the support costs.  
All security components at the client level are from a single security vendor, which is less expensive than managing several security products from multiple vendors. Since all components are from a single vendor and can be installed, updated, and reported on from same place, Symantec Endpoint Protection eliminates cross-vendor interoperability issues.

Symantec Endpoint Protection is available through the Symantec network of corporate resellers and national distributors.

## About Symantec Endpoint Protection

Symantec Endpoint Protection protects endpoint computing devices from virus threats and risks, and provides three layers of protection to your endpoint computing devices. The layers are Network Threat Protection, Proactive Threat Protection, and Antivirus and Antispyware Protection.

**Figure 1-1** Protection layers

Network Threat Protection blocks threats from your computer by using rules and signatures. Proactive Threat Protection identifies and mitigates the threats that are based on the threat's behavior. Antivirus and Antispyware Protection identifies and mitigates the threats that try to or have gained access to your computers by using the signatures that Symantec creates.

## About Network Threat Protection

Network Threat Protection consists of firewall and intrusion prevention software to protect your endpoint computing devices. The firewall supports the rules that are written for both specific ports and specific applications, and uses stateful inspection of all network traffic. Therefore, for all network traffic that is client-initiated, you only have to create an outbound rule to support that traffic. Stateful inspection automatically permits the return traffic that responds to the outbound traffic.

The firewall provides full support for TCP, UDP, ICMP, and all IP protocols such as ICMP and RSVP. The firewall also supports Ethernet and Token Ring protocols, and can block protocol drivers such as VMware and WinPcap. The firewall can automatically recognize legitimate DNS, DHCP, and WINS traffic, so you can check a check box to permit this traffic without writing rules.

---

**Note:** Symantec assumes that you construct your firewall rules such that all traffic that is not permitted is denied. The firewall does not support IPv6.

---

The intrusion prevention engine supports checking for port scans and denial-of-service attacks, and protects against buffer overflow attacks. This engine also supports the automatic blocking of malicious traffic from infected computers.

The intrusion detection engine supports deep packet inspection, regular expressions, and lets you create custom signatures.

## About Proactive Threat Protection

Proactive Threat Protection identifies threats, such as worms, viruses, Trojan horses, and programs that log keystrokes based on the behavior of processes on the computer. TruScan proactive threat scans identify these threats by their actions and characteristics, not by traditional security signatures. Proactive threat scans analyze the threat's behavior against hundreds of detection modules to determine whether the active processes are safe or malicious. This technology can immediately detect and mitigate the unknown threats by their behavior without traditional signatures or patches.

On supported 32-bit operating systems, Proactive Threat Protection also lets you control read, write, and execute access to hardware devices, files, and registry keys. If necessary, you can refine the control to specific, supported operating systems. You can also block peripheral devices by class ID such as USB, Bluetooth, infrared, FireWire, serial, parallel, SCSI, and PCMCIA.

## About Antivirus and Antispyware Threat Protection

Antivirus and Antispyware Threat Protection prevents infections on computers by scanning the boot sector, memory, and files for viruses, spyware, and security risks. Antivirus and Antispyware Threat Protection uses the virus and the security risk signatures that are found in virus definitions files. This protection also protects your computers by blocking security risks before they can install if doing so would not leave the computer in an unstable state.

Antivirus and Antispyware Threat Protection includes Auto-Protect, which detects viruses and security risks when they try to access memory or install themselves. Auto-Protect also scans for security risks such as adware and spyware. When it finds security risks, it quarantines the infected files, or removes and repairs the side effects of the security risks. You can also disable scanning for security risks in Auto-Protect. Auto-Protect can repair complicated risks, such as sheathed user mode risks (rootkits). Auto-Protect can also repair the persistent security risks that are difficult to remove or that reinstall themselves.

Antivirus and Antispyware Threat Protection also includes Auto-Protect scanning for Internet email programs by monitoring all POP3 and SMTP traffic. You can configure Antivirus and Antispyware Threat Protection to scan incoming messages for threats and security risks, as well as outgoing messages for known heuristics. Scanning outgoing email helps to prevent the spread of threats such as worms that can use email clients to replicate across a network.

---

**Note:** Auto-Protect for Web-based Internet email programs is blocked from installation on server-based operating systems. For example, you cannot install this feature on Windows Server 2003.

---

## About Symantec

Symantec is a global leader in infrastructure software. Symantec enables businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and the services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at the following URL:

[www.symantec.com](http://www.symantec.com)



# Installing Symantec Endpoint Protection

This chapter includes the following topics:

- [System installation requirements](#)
- [Installation process overview](#)
- [About Desktop firewalls and communications ports](#)
- [Installing and configuring Symantec Endpoint Protection Manager](#)
- [Logging on to the Symantec Endpoint Protection Manager Console](#)

## System installation requirements

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

---

**Note:** Installation to or from the directory names that contain double-byte characters is not supported.

---

## Symantec Endpoint Protection Manager, Console, and database

[Table 2-1](#) lists the minimum requirements for the computers on which to install the Symantec Endpoint Protection Manager and Console, and the database.

**Table 2-1** Symantec Endpoint Protection Manager, Console, and database

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III	1 GHz on x64 works only with the following processors: <ul style="list-style-type: none"> <li>■ Intel Xeon with Intel EM64T support</li> <li>■ Intel Pentium IV with EM64T support</li> <li>■ AMD 64-bit Opteron</li> <li>■ AMD 64-bit Athlon</li> </ul> <b>Note:</b> Itanium is not supported.
Operating system	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> <li>■ Windows 2000 Server/Advanced Server/Datacenter Server/Small Business Server with Service Pack 3 or later</li> <li>■ Windows XP Professional with Service Pack 1 or later</li> </ul> <p><b>Note:</b> Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for <i>Symantec Endpoint Protection Manager 11.x communication troubleshooting</i> on the <a href="#">Symantec Support Web Site</a>.</p> <ul style="list-style-type: none"> <li>■ Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Storage Edition/Web Edition/Small Business Server</li> </ul>	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> <li>■ Windows XP Professional x64 Edition with Service Pack 1 or later</li> <li>■ Windows Server 2003 Standard x64 Edition/Enterprise x64 Edition/Datacenter x64 Edition with Service Pack 1 or later</li> <li>■ Windows Compute Cluster Server 2003</li> <li>■ Windows Storage Server 2003</li> </ul> <p><b>Note:</b> If you use Microsoft Clustering services for the Symantec Endpoint Protection Manager server, you must install the Symantec Endpoint Protection Manager on the local volume.</p>
Memory	1 GB RAM minimum (2-4 GB recommended)	1 GB RAM minimum (2-4 GB recommended)
Hard disk	4 GB for the server, plus an additional 4 GB for the database	4 GB for the server, plus an additional 4 GB for the database
Display	Super VGA (1,024x768) or higher resolution video adapter and monitor	Super VGA (1,024x768) or higher resolution video adapter and monitor

**Table 2-1** Symantec Endpoint Protection Manager, Console, and database  
*(continued)*

Component	32-bit	64-bit
Database	<p>The Symantec Endpoint Protection Manager includes an embedded database.</p> <p>You may also choose to use one of the following versions of Microsoft SQL Server:</p> <ul style="list-style-type: none"> <li>■ Microsoft SQL Server 2000 with Service Pack 3 or later</li> <li>■ Microsoft SQL Server 2005</li> </ul> <p><b>Note:</b> Microsoft SQL Server is optional.</p>	<p>The Symantec Endpoint Protection Manager includes an embedded database.</p> <p>You may also choose to use one of the following versions of Microsoft SQL Server:</p> <ul style="list-style-type: none"> <li>■ Microsoft SQL Server 2000 with Service Pack 3 or later</li> <li>■ Microsoft SQL Server 2005</li> </ul> <p><b>Note:</b> Microsoft SQL Server is optional.</p>
Other requirements	<p>The following other requirements must be met:</p> <ul style="list-style-type: none"> <li>■ Internet Information Services server 5.0 or later with World Wide Web services enabled</li> <li>■ Internet Explorer 6.0 or later</li> <li>■ Static IP address (recommended)</li> </ul>	<p>The following other requirements must be met:</p> <ul style="list-style-type: none"> <li>■ Internet Information Services server 5.0 or later with World Wide Web services enabled</li> <li>■ Internet Explorer 6.0 or later</li> <li>■ Static IP address (recommended)</li> </ul>

## Symantec Endpoint Protection Manager and Console

[Table 2-2](#) lists the minimum requirements for the computers on which to install the Symantec Endpoint Protection Manager and Console.

**Table 2-2** Symantec Endpoint Protection Manager and Console

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III	<p>1 GHz on x64 works only with the following processors:</p> <ul style="list-style-type: none"> <li>■ Intel Xeon with Intel EM64T support</li> <li>■ Intel Pentium IV with EM64T support</li> <li>■ AMD 64-bit Opteron</li> <li>■ AMD 64-bit Athlon</li> </ul> <p><b>Note:</b> Itanium is not supported.</p>

**Table 2-2** Symantec Endpoint Protection Manager and Console (*continued*)

Component	32-bit	64-bit
Operating system	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> <li>■ Windows 2000 Server/Advanced Server/Datacenter Server with Service Pack 3 or later</li> <li>■ Windows XP Professional with Service Pack 1 or later</li> </ul> <p><b>Note:</b> Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for <i>Symantec Endpoint Protection Manager 11.x communication troubleshooting</i> on the <a href="#">Symantec Support Web Site</a>.</p> <ul style="list-style-type: none"> <li>■ Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition/Small Business Server</li> </ul>	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> <li>■ Windows XP Professional x64 Edition with Service Pack 1 or later</li> <li>■ Windows Server 2003 Standard x64 Edition/Enterprise x64 Edition/Datacenter x64 Edition with Service Pack 1 or later</li> <li>■ Windows Compute Cluster Server 2003</li> <li>■ Windows Storage Server 2003</li> </ul> <p><b>Note:</b> If you use Microsoft Clustering services for the Symantec Endpoint Protection Manager server, you must install the SEPM server on the local volume.</p>
Memory	1 GB of RAM minimum (2 GB recommended)	1 GB of RAM (2 GB recommended)
Hard disk	2 GB (4 GB recommended)	2 GB (4 GB recommended)
Display	Super VGA (1,024x768) or higher resolution video adapter and monitor	Super VGA (1,024x768) or higher resolution video adapter and monitor
Other requirements	<p>The following other requirements must be met:</p> <ul style="list-style-type: none"> <li>■ Internet Information Services server 5.0 or later with World Wide Web services enabled</li> <li>■ Internet Explorer 6.0 or later</li> <li>■ Static IP address (recommended)</li> </ul>	<p>The following other requirements must be met:</p> <ul style="list-style-type: none"> <li>■ Internet Information Services server 5.0 or later with World Wide Web services enabled</li> <li>■ Internet Explorer 6.0 or later</li> <li>■ Static IP address (recommended)</li> </ul>

## Symantec Endpoint Protection Console

[Table 2-3](#) lists the minimum requirements for the computers on which to install the Symantec Endpoint Protection Console.

**Table 2-3** Symantec Endpoint Protection Console

Component	32-bit	64-bit
Processor	1 GHz Intel Pentium III	1 GHz on x64 works only with the following processors: <ul style="list-style-type: none"> <li>■ Intel Xeon with Intel EM64T support</li> <li>■ Intel Pentium IV with EM64T support</li> <li>■ AMD 64-bit Opteron</li> <li>■ AMD 64-bit Athlon</li> </ul> <b>Note:</b> Itanium is not supported.
Operating system	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> <li>■ Windows 2000 Professional/Server/Advanced Server/Datacenter Server/Small Business Server with Service Pack 3 or later</li> <li>■ Windows XP Professional with Service Pack 1 or later</li> </ul> <p><b>Note:</b> Windows XP supports a limited number of concurrent users if the clients are in "push" mode. Use "pull" mode on Windows XP servers for up to 100 clients. For more information, search for <i>Symantec Endpoint Protection Manager 11.x communication troubleshooting</i> on the <a href="#">Symantec Support Web Site</a>.</p> <ul style="list-style-type: none"> <li>■ Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition/Small Business Server</li> <li>■ Windows Vista (x86)</li> </ul>	<p>The following operating systems are supported:</p> <ul style="list-style-type: none"> <li>■ Windows XP Professional x64 Edition with Service Pack 1 or later</li> <li>■ Windows Server 2003 Standard x64 Edition/Enterprise x64 Edition/Datacenter x64 Edition with Service Pack 1 or later</li> <li>■ Windows Compute Cluster Server 2003</li> <li>■ Windows Storage Server 2003</li> <li>■ Windows Vista (x64)</li> </ul> <p><b>Note:</b> If you use Microsoft Clustering services for the Symantec Endpoint Protection Manager server, you must install the Symantec Endpoint Protection Manager server on the local volume.</p>
Memory	512 MB of RAM (1 GB recommended)	512 MB of RAM (1 GB recommended)
Hard disk	15 MB	15 MB
Display	Super VGA (1,024x768) or higher resolution video adapter and monitor	Super VGA (1,024x768) or higher resolution video adapter and monitor
Browser	<ul style="list-style-type: none"> <li>■ Internet Explorer 6.0 or later</li> </ul>	<ul style="list-style-type: none"> <li>■ Internet Explorer 6.0 or later</li> </ul>

## Symantec Endpoint Protection

Table 2-4 lists the minimum requirements for the computers on which to install Symantec Endpoint Protection.

**Table 2-4** Symantec Endpoint Protection

Component	32-bit	64-bit
Processor	400 MHz Intel Pentium III (1 GHz for Windows Vista)	1 GHz on x64 only with the following processors: <ul style="list-style-type: none"> <li>■ Intel Xeon with Intel EM64T support</li> <li>■ Intel Pentium IV with EM64T support</li> <li>■ AMD 64-bit Opteron</li> <li>■ AMD 64-bit Athlon</li> </ul> <p><b>Note:</b> Itanium is not supported.</p>
Operating system	The following operating systems are supported: <ul style="list-style-type: none"> <li>■ Windows 2000 Professional/Server/Advanced Server/Datacenter Server/Small Business Server with Service Pack 3 or later</li> <li>■ Windows XP Home Edition/Professional Edition/Tablet PC Edition/Media Center Edition</li> <li>■ Windows Server 2003 Standard Edition/Enterprise Edition/Datacenter Edition/Web Edition/Small Business Server</li> <li>■ Windows Vista (x86) Home Basic Edition/Home Premium Edition/Business Edition/Enterprise Edition/Ultimate Edition</li> <li>■ Windows Server 2008 Standard Edition/Enterprise Edition/ Datacenter Edition/Web Edition (Core and Full)</li> </ul>	The following operating systems are supported: <ul style="list-style-type: none"> <li>■ Windows XP Professional x64 Edition</li> <li>■ Windows Server 2003 x64 Edition</li> <li>■ Windows Compute Cluster Server 2003</li> <li>■ Windows Storage Server 2003</li> <li>■ Windows Vista Home Basic x64 Edition/Home Premium x64 Edition/Business x64 Edition/Enterprise x64 Edition/Ultimate x64 Edition</li> <li>■ Windows Server 2008 Standard x64 Edition/Enterprise x64 Edition/ Datacenter x64 Edition/Web x64 Edition (Core and Full)</li> </ul> <p><b>Note:</b> If you use Microsoft Clustering Services, you must install the client on the local volume.</p>
Memory	256 MB of RAM	256 MB of RAM
Hard disk	600 MB	700 MB
Display	Super VGA (1,024x768) or higher-resolution video adapter and monitor	Super VGA (1,024x768) or higher-resolution video adapter and monitor

**Table 2-4** Symantec Endpoint Protection (continued)

Component	32-bit	64-bit
Other requirements	Internet Explorer 6.0 or later  Terminal Server clients connecting to a computer with antivirus protection have the following additional requirements: <ul style="list-style-type: none"> <li>■ Microsoft Terminal Server RDP (Remote Desktop Protocol) client</li> <li>■ Citrix Metaframe (ICA) client 1.8 or later if using Citrix Metaframe server on Terminal Server</li> </ul>	Internet Explorer 6.0 or later

---

**Note:** The Push Deployment Wizard does not check to verify that Internet Explorer 6.0 or later is installed on computers when it is required. If the target computers do not have the correct version of Internet Explorer, the installation fails without informing you.

---

## Installation process overview

The *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* contains detailed information about each procedure in the installation process.

[Table 2-5](#) summarizes the process to install Symantec Endpoint Protection.

**Table 2-5** Installation overview

Procedure	Description
Install Symantec Endpoint Protection Manager	Decide on the computer to which you want to install the software and the type of database that you want to use. Then, run the installation program from the CD. The program first installs the manager software. It then installs and configures the database.  See <a href="#">“Installing and configuring Symantec Endpoint Protection Manager”</a> on page 27.

**Table 2-5** Installation overview (*continued*)

Procedure	Description
Create a client install package	<p>For your test environment you can create and install default client software packages. Those clients are assigned to the Temporary group and use the default policies.</p> <p>If there are a large number of computers in your production environment, you may want to create custom security policies first. You can then create custom client installation packages before deploying to the clients.</p> <p>At the end of the database configuration, you are asked if you want to run the Migration and Deployment Wizard. This wizard creates and then pushes out a default client software installation package.</p> <p>See <a href="#">“Creating client installation packages”</a> on page 105.</p>
Deploy the client software	<p>Decide how you want to deploy the client software. You can deploy the client software in several different ways. For ease of use, you can use the Migration and Deployment Wizard after you install the manager to deploy the default protection. Alternately, you can use the Migration and Deployment Wizard from the Start menu at any time.</p>
Log on to Symantec Endpoint Protection Manager console	<p>To log on, you can use the Start menu and the admin user name, with the password that you set during installation.</p> <p>See <a href="#">“Logging on to the Symantec Endpoint Protection Manager Console”</a> on page 42.</p>
Locate your group in the console	<p>On the Clients page, the group that you created when you installed appears under View Clients.</p>
Configure LiveUpdate for site updates	<p>You need to configure LiveUpdate properties for the site you have installed.</p> <p>See <a href="#">“About LiveUpdate Policies”</a> on page 49.</p>
Configure LiveUpdate for client updates	<p>After you configure the site, you need to configure a LiveUpdate Settings Policy and a LiveUpdate Content Policy for your clients.</p> <p>See <a href="#">“About LiveUpdate Policies”</a> on page 49.</p>
Configure security policies and test Symantec Endpoint Protection	<p>At a minimum, you should configure and test an Antivirus and Antispyware Policy for your clients. You may also want to configure a Firewall Policy and policies for the other types of protection.</p> <p>See <a href="#">“Evaluating policies”</a> on page 55.</p>

## About Desktop firewalls and communications ports

If your servers and clients run firewall software, you must open certain ports so that communication between the management servers and clients is possible. Alternatively, you can permit the application Rtvscan.exe on all computers to

send and receive traffic through your firewalls. Also, remote server and client installation tools require that TCP port 139 be opened.

---

**Note:** Management servers and clients use the default ephemeral port range for TCP (1024 to 65535) for network communications. The ephemeral port range that is used, however, rarely exceeds 5,000. The ephemeral port range is configurable for most operating systems. Most firewalls use stateful inspection when filtering TCP traffic, so incoming TCP responses are automatically allowed and routed back to the original requester. Therefore you do not have to open the ephemeral TCP ports when you configure your firewall software.

---

[Table 2-6](#) lists the network protocols and ports that management servers and clients require for communicating and network installations.

**Table 2-6** Ports for client and server installation and communication

Function	Component	Protocol and port
Push Deployment Wizard deployment	Symantec Endpoint Protection Managers and clients	TCP 139 and 445 on managers and clients  UDP 137 and 138 on managers and clients  TCP ephemeral ports on servers and clients
Network Audit	Symantec Endpoint Protection Managers and clients	TCP 139 and 445 on managers  TCP ephemeral ports on clients
Group Update Provider communication	Symantec Endpoint Protection Managers and Group Update Providers  Group Update Providers and clients	TCP 2967 on all devices  <b>Note:</b> This port is the default, which can be changed.
General communication	Symantec Endpoint Protection Managers and clients	TCP 80 on managers  TCP ephemeral ports on clients  <b>Note:</b> Port 80 can also be changed to TCP 443 (HTTPS).

**Table 2-6** Ports for client and server installation and communication  
*(continued)*

Function	Component	Protocol and port
General communication	Remote Symantec Endpoint Protection Manager Consoles and Symantec Endpoint Protection Managers	TCP 8443 on managers TCP ephemeral ports and 9090 on consoles <b>Note:</b> This port number is configurable.
Replication communication	Site to site between database servers	TCP 8443 between database servers
Remote Symantec Endpoint Protection Manager Console installation	Symantec Endpoint Protection Manager and remote Symantec Endpoint Protection Manager Console	TCP 9090 on remote managers TCP ephemeral ports on remote consoles <b>Note:</b> This port number is configurable.
External database communication	Remote Microsoft SQL servers and Symantec Endpoint Protection Managers	TCP 1433 on remote Microsoft SQL servers TCP ephemeral ports on managers <b>Note:</b> Port 1433 is the default port.
Symantec Network Access Control Enforcer communication	Symantec Endpoint Protection Manager and Enforcer	TCP 1812 on managers TCP Ephemeral ports on enforcers <b>Note:</b> RADIUS servers also use port 1812, so do not install Symantec Endpoint Protection Manager on the same server. This port is not configurable on Symantec Endpoint Protection Manager.

**Table 2-6** Ports for client and server installation and communication  
(continued)

Function	Component	Protocol and port
Migration and Deployment Wizard	Symantec Endpoint Protection Manager and legacy Symantec management servers	TCP 139, TCP 445, TCP ephemeral ports, and UDP 137 on managers  TCP 139, TCP 445, TCP ephemeral ports, and UDP 137 on legacy Symantec management servers
LiveUpdate	LiveUpdate clients and servers	TCP ephemeral ports on clients  TCP 80 on LiveUpdate servers

## Installing and configuring Symantec Endpoint Protection Manager

Installing management software for the first time is divided into two parts. The first part installs Symantec Endpoint Protection Manager. The second part installs and configures the Symantec Endpoint Protection Manager database. In the first, you can accept all defaults. In the second part, you must select the type of configuration you want for the Symantec Endpoint Protection Manager, Simple or Advanced, based on the number of clients the server supports. The Simple configuration, intended for a server that supports less than 100 clients, automatically creates an embedded database and uses the default values for most settings with minimal input from you. The Advanced configuration, intended for administrators in larger environments, lets you specify settings specific to your environment.

---

**Note:** Management software does not include Symantec Endpoint Protection or any other client software that is managed.

---

### To install Symantec Endpoint Protection Manager

- 1 Insert the installation CD and start the installation if it does not start automatically.
- 2 In the Welcome panel do one of the following:
  - To install for Symantec Endpoint Protection, click **Install Symantec Endpoint Protection Manager**.

- To install for Symantec Network Access Control, click **Install Symantec Network Access Control**, and then click **Install Symantec Endpoint Protection Manager** on the next panel.
- 3 In the Welcome panel, click **Next**.
  - 4 In the License Agreement panel, check **I accept the terms in the license agreement**, and then click **Next**.
  - 5 In the Destination Folder panel, accept or change the installation directory.
  - 6 Do one of the following:
    - To let the Symantec Endpoint Protection Manager IIS Web server run with other Web servers on this computer, check **Use the default Web site**, and then click **Next**.
    - To configure the Symantec Endpoint Protection Manager IIS Web as the only Web server on this computer, check **Create a custom Web site**, and then click **Next**.
  - 7 In the Ready to Install panel, click **Install**.
  - 8 When the installation finishes and the Install Wizard Complete panel appears, click **Finish**.

Wait for the Management Server Configuration Wizard panel to appear, which can take up to 15 additional seconds. Perform the steps in the following section appropriate to the configuration type you selected, Simple or Advanced.

### To configure Symantec Endpoint Protection Manager in Simple Mode

- 1 In the Management Server Configuration Wizard panel select **Simple**, and then click **Next**.

A system check is performed to determine if the system meets the minimal requirements for available memory and drive space. If it does not, a warning dialog is displayed indicating that the server may not perform as expected with the resources available. You can choose to continue or cancel the configuration.

- 2 Specify and confirm a password (of 6 or more characters). Optionally, provide an email address.

The password specified is used for the Symantec Endpoint Protection Manager admin account, as well as the encryption password necessary for disaster recovery. After installation, the encryption password does not change, even if the password for the admin account is changed.

Document this password when you install Symantec Endpoint Protection in your production environment. You need it for disaster recovery purposes and for adding optional Enforcer hardware.

Symantec Endpoint Protection Manager sends warning and notification messages to the email address that you provide.

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

### To configure Symantec Endpoint Protection Manager in Advanced Mode

- 1 In the Management Server Configuration Wizard panel select **Advanced**, and then click **Next**.

- 2 Select the number of clients you plan to have managed by this server, and then click **Next**.

A system check is performed to determine if the system meets the minimal requirements for available memory and drive space. If it does not, a warning dialog is displayed indicating that the server may not perform as expected with the resources available. You can choose to continue or cancel the configuration.

- 3 In the Site Type panel, check **Install my first Site**, and then click **Next**.
- 4 In the Server Information panel, accept or change the default values for the following boxes, and then click **Next**:

- Server name

- Server port
  - Web console port
  - Server data folder
- 5 In the Site Name panel, in the Site name box, enter your site name, and then click **Next**.
  - 6 In the Encryption Password panel, type a value in both boxes, and then click **Next**.

Document this password when you install Symantec Endpoint Protection in your production environment. You need it for disaster recovery purposes and for adding optional Enforcer hardware.
  - 7 In the Database Server Choice panel, check **Embedded Database**, and then click **Next**.
  - 8 On the admin user panel, in the Password boxes, type a password for the admin account to log on to the console. Optionally, provide an email address.

Symantec Endpoint Protection Manager sends warning and notification messages to the email address specified.

When the installation finishes, you have the option of deploying client software with the Migration and Deployment Wizard. If you do not deploy client software at this time, refer to the Client Installation chapter for details on how to install client software. Log on to the console with the user name and password that you entered here.
  - 9 Click **Next**.

## Installing Symantec Endpoint Protection Manager with an embedded database

Installing with the embedded database is the easiest way to install Symantec Endpoint Protection Manager. The embedded database supports up to 5,000 clients. After you install Symantec Endpoint Protection Manager and become comfortable with administration tasks, you must secure your cryptographic files in case you need to recover from a disaster. You must also document the encryption password that you enter during Symantec Endpoint Protection Manager configuration.

## Installing Symantec Endpoint Protection Manager with a Microsoft SQL database

You can install the Symantec Endpoint Protection Manager on the same computer that runs Microsoft SQL Server 2000/2005 and then create a database on the local

SQL server. You can also install the Symantec Endpoint Protection Manager on a computer that does not run Microsoft SQL Server 2000/2005 and then create a database on the remote SQL server. In both cases, you must properly install and configure Microsoft SQL Server components on all computers.

---

**Note:** Microsoft SQL Server 2000 is supported on English-language Windows operating systems only.

---

## Preparing Microsoft SQL Server 2000/2005 for database creation

Before you create the database, Symantec recommends that you install a new instance of SQL Server that conforms to Symantec installation and configuration requirements. You can install a database in an older, existing instance, but the instance must be configured properly or your database installation fails. For example, if the authentication configuration is not set to Mixed Mode, your installation fails or does not function properly. If you select a case-sensitive SQL collation your installation fails.

---

**Warning:** Symantec Endpoint Protection Manager authenticates to Microsoft SQL Server with a clear text database owner user name and password. If you install to and communicate with a remote Microsoft SQL Server, any computer in the communications path can potentially capture this user name and password with a packet capture utility. To maximize the security posture of remote Microsoft SQL Server communications, collocate both servers in a secure subnet.

---

A secure subnet isolates network communications between servers to that subnet only. A secure subnet is typically located behind a network device that performs network address translation (NAT). Many of the modern inexpensive routers that perform DHCP address assignments also perform NAT. A secure subnet is also physically secure so that only authorized personnel have physical access to the network devices on that subnet.

## Microsoft SQL Server 2000 installation and configuration requirements

The installation and configuration requirements affect all Microsoft SQL Server 2000 installations, both local and remote. To create a database on a remote SQL server, you must also install the SQL Server Client Components on the server that runs the Symantec Endpoint Protection Manager.

### Microsoft SQL Server 2000 installation requirements

When you install the instance of Microsoft SQL Server 2000, select the following non-default features:

- Do not accept the default instance name. Use SEPM or some other name.  
By default, a database named Sem5 is created in this instance when you install the Symantec Endpoint Protection Manager. The default instance is supported, which is unnamed, but can lead to confusion if you install multiple instances on one computer.
- Set authentication configuration to Mixed Mode (Windows authentication and SQL Server authentication).
- Set the sa password when you set Mixed Mode authentication. You type this password when you install the Symantec Endpoint Protection Manager.

---

**Note:** When you install the instance of Microsoft SQL Server, do not select a case-sensitive SQL collation. The database does not support case-sensitivity.

---

### Microsoft SQL Server 2000 configuration requirements

After you install the instance of Microsoft SQL Server 2000, you must do the following:

- Apply SQL Server Service Pack 4, and select to authenticate using SQL server credentials.
- In Enterprise Manager, register the instance, right-click the instance, and edit the registration properties to use SQL server authentication.
- After editing, when prompted, disconnect from the server.
- Right-click the instance and connect to the server.
- Use the SQL Server Network Utility to verify that TCP/IP is an enabled protocol. If the protocol is not enabled, enable the protocol.
- Verify that SQL Server Agent is running, and start it if it is not running.

### Installing and configuring Microsoft SQL Server 2000 client components

You install and configure Microsoft SQL Server 2000 Client Components on the computer that runs or will run the Symantec Endpoint Protection Manager.

### To install Microsoft SQL Server 2000 client components

- 1 Start the Microsoft SQL Server 2000 installation CD and begin the installation process.
- 2 In the Installation Definition window, click **Client Tools Only**.
- 3 Complete the installation.

### To configure Microsoft SQL Server 2000 client components

- 1 Click **Start > Programs > Microsoft SQL Server > Client Network Utility**.
- 2 In the SQL Server Client Network Utility dialog box, on the General tab, verify that TCP/IP is an enabled protocol. If it is not an enabled protocol, enable the protocol.
- 3 Right-click **TCP/IP**, and then click **Properties**.
- 4 In the TCP/IP dialog box, in the Default Port box, type the port number that matches the port that is used by the Microsoft SQL Server 2000 instance.  
  
The default port is typically 1433. You specify this port number when you create the database.
- 5 Click **OK**, and then exit the SQL Server Client Network Utility.

### Microsoft SQL Server 2005 installation and configuration requirements

The installation and configuration requirements affect all Microsoft SQL Server 2005 installations, both local and remote. If you create a database on a remote SQL server, you must also install the SQL Server Client Components on the server that runs the Symantec Endpoint Protection Manager.

### Microsoft SQL Server 2005 installation requirements

When you install the instance of Microsoft SQL Server 2005 you must select the following non-default features:

- Do not accept the default instance name. Use SEPM or some other name.  
By default, a database named Sem5 is created in this instance when you install the Symantec Endpoint Protection Manager. The default instance is supported, which is unnamed, but can lead to confusion if you install multiple instances on one computer.
- Set authentication configuration to Mixed Mode (Windows authentication and SQL Server authentication).
- Set the sa password when you set Mixed Mode authentication. You type this password when you install the Symantec Endpoint Protection Manager.
- When you configure Service Accounts, select to start the SQL Server Browser at the end of setup.

---

**Note:** When you install the instance of Microsoft SQL Server, do not select a case-sensitive SQL collation. The database does not support case-sensitivity.

---

### Microsoft SQL Server 2005 configuration requirements

After you install the instance of Microsoft SQL Server 2005, apply SQL Server 2005 Service Pack 2, and select to authenticate using SQL server credentials. Then, use the SQL Server Configuration Manager to do the following:

- Display the protocols for the SQL Server 2005 Network Configuration.
- Display the protocol properties for TCP/IP and enable TCP/IP.
- Display the IP addresses for TCP/IP and enable the IP1 and IP2 addresses.
- Set the TCP/IP port numbers for IP1, IP2, and PALL.

The Symantec Endpoint Protection Manager database does not support dynamic ports. As a result, set TCP Dynamic Ports to blank, and specify a TCP Port number. The default is typically 1433. You specify this port number when you create the database.

- Restart the SQL Server service.

If you did not select to start the SQL Browser during installation, your remote installation fails. If you did not make this selection during installation, use the SQL Server Surface Area Configuration utility to do the following:

- Display the Surface Area Configuration for Services and Connections information.
- Enable the SQL Server Browser service.  
If this service is not enabled, client computers cannot communicate with the server.
- Verify that Local and Remote Connections are enabled by using TCP/IP only. Named Pipes are not required.

### Installing and configuring Microsoft SQL Server 2005 client components

You install Microsoft SQL Server 2005 client components on the computer that runs the Symantec Endpoint Protection Manager.

---

**Note:** You must install the client components on a computer that runs Windows Server 2003. The client component installation requires MDAC 2.8 Service Pack 1 or higher, Windows Installer 3.1, and Internet Explorer 6.0 Service Pack 1 or higher.

---

### To install Microsoft SQL Server 2005 client components

- 1 Start the Microsoft SQL Server 2005 installation CD and begin the installation process.
- 2 In the Start window, click **Server components, tools, Books Online, and samples**.
- 3 Continue the installation until you are prompted to select the components to install.
- 4 In the Components to Install dialog box, click **Advanced**.
- 5 In the left pane, click and expand **Client Components**.
- 6 Click **Client Components**, and then select **Will be installed on local hard drive**.
- 7 Click the following Client Component features: **Connectivity Components** and **Management Tools**, and then select **Will be installed on local hard drive**.
- 8 Complete the installation.

### To configure Microsoft SQL Server 2005 client components

- 1 Click **Start > Programs > Microsoft SQL Server 2005 > Configuration Tools > SQL Server Configuration Manager**.
- 2 Under SQL Native Client Configuration, click **Client Protocols**, right-click **TCP/IP**, and then click **Properties**.
- 3 In the Default Port box, type the port number that matches the port that is used by the Microsoft SQL Server 2005 instance.  
  
The default port is typically 1433. You specify this port number when you create the database.
- 4 Click **Apply > OK**.

## SQL Server requirements for installing Symantec Endpoint Protection Manager

If you install Symantec Endpoint Protection Manager with a Microsoft SQL Server database, there are specific configuration requirements for SQL Server. You can install Symantec Endpoint Protection Manager with either a local database or a remote database.

[Table 2-7](#) describes the SQL Server configuration settings that Symantec Endpoint Protection Manager requires.

**Table 2-7** SQL server configuration requirements

Configuration setting	Symantec Endpoint Protection Manager installation requirement
Instance name	Do not use the default name. Create a name such as SEPM.  By default, a database named Sem5 is created in the SQL Server instance when you install the Symantec Endpoint Protection Manager. The default instance is unnamed. It is supported, but can cause confusion if you install multiple instances on one computer.
Authentication configuration	Mixed Mode
sa password	Set this password when you set Mixed Mode authentication.
Authentication	SQL Server authentication
Enabled protocol	TCP/IP
IP addresses for TCP/IP (SQL Server 2005 only)	Enable IP1 and IP2
TCP/IP port numbers for IP1, IP2, and PALL (SQL Server 2005 only)	Set TCP Dynamic Ports to blank, and specify a TCP Port number. The default is typically 1433. You specify this port number when you create the database.  The Symantec Endpoint Protection Manager database does not support dynamic ports.
SQL Server Browser service (SQL Server 2005 only)	Must be started.

If your database is located on a remote server, you must also install SQL Server client components on the computer that runs Symantec Endpoint Protection Manager.

During Symantec Endpoint Protection Manager installation, you make decisions about what database values to set. You should make these decisions before you start the installation.

[Table 2-8](#) lists and describes these values and settings.

**Table 2-8** Settings for installing Symantec Endpoint Protection Manager with a SQL Server database

Setting	Default	Description
Select IIS Web site configuration options	Use the default Web site	<ul style="list-style-type: none"> <li>■ Use the default Web site Installs the Symantec Endpoint Protection IIS Web application in the default IIS Web site, and works with any other Web application that is installed in the Web site.</li> <li>■ Create a custom Web site Disables the default IIS Web site, and creates a Symantec Web server for Symantec Endpoint Protection Manager.</li> </ul>
Server name	<i>local host name</i>	Name of the computer that runs the Symantec Endpoint Protection Manager.
Server port	8443	Port number on which the Symantec Endpoint Protection Manager server listens.
Web console port	9090	HTTP port used for remote console connections
Server data folder	C:\Program Files\Symantec Endpoint Protection Manager\data	Directory in which the Symantec Endpoint Protection Manager places data files including backups, replication, and other Symantec Endpoint Protection Manager files. The installer creates this directory if it does not exist.
Site name	Site <i>local host name</i>	Site name of the highest level container under which all features are configured and run with the Symantec Endpoint Protection Manager.
Encryption password	None	<p>The password that encrypts communication between the Symantec Endpoint Protection Manager, clients, and optional Enforcer hardware devices. The password can be from 1-32 alphanumeric characters and is required.</p> <p>Document this password and put it in a secure location. You cannot change or recover the password after you create the database. You must also enter this password for disaster recovery purposes if you do not have a backed up database to restore.</p>

**Table 2-8** Settings for installing Symantec Endpoint Protection Manager with a SQL Server database (*continued*)

Setting	Default	Description
Database server	<i>local host name</i>	Name of the Microsoft SQL server and the optional instance name. If the database server was installed with the default instance, which is no name, type either <i>host name</i> or the host's <i>IP address</i> . If the database server was installed with a named instance, type either <i>host name\instance_name</i> or <i>IP address\instance_name</i> . Typing <i>host name</i> only works with properly configured DNS.  If you install to a remote database server, you must first install the SQL Server client components on the computer that runs the Symantec Endpoint Protection Manager.
SQL Server Port	1433	Port that the computer running SQL Server is configured with to send and receive traffic.  Port 0, which is used to specify a random, negotiated port, is not supported.
Database Name	sem5	Name of the database that is created.
User	sem5	Name of the database user account that is created. The user account has a standard role with read and write access. The name can be a combination of alphanumeric values and the special characters ~#%_+= :./ . The special characters `!@\${^&*()-{}[]\<>;>,? are not allowed. The following names are also not allowed: sysadmin, server admin, setupadmin, securityadmin, processadmin, dbcreator, diskadmin, bulkadmin.
Password	None	The password to associate with the database user account. The name can be a combination of alphanumeric values and the special characters ~#%_+= :./ . The special characters `!@\${^&*()-{}[]\<>;>,? are not allowed.
SQL client folder	C:\Program Files\Microsoft SQL Server\80\Tools\Binn	Location of the local SQL Client Utility directory that contains bcp.exe.  If you create a database on SQL Server 2005, the default numeric directory is 90. The complete default path is C:\Program Files\Microsoft SQL Server\90\Tools\Binn
DBA user	None	Name of the database server administrator account, which is typically sa.

**Table 2-8** Settings for installing Symantec Endpoint Protection Manager with a SQL Server database (*continued*)

Setting	Default	Description
DBA password	None	Name of the password that is associated with the database user account.
Database data folder	Automatically detected after clicking Default  SQL Server 2000: C:\Program Files\Microsoft SQL Server\MSSQL\Data  SQL Server 2005: C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data	Location of the SQL Server data directory. If you install to a remote server, the volume identifier must match the identifier on the remote server. If you are installing to a named instance on SQL Server 2000, the instance name is appended to MSSQL with a dollar sign as in \MSSQL\$ <i>instance name</i> \Data. If you are installing to a named instance on SQL Server 2005, the instance name is appended to MSSQL with a dot numeric identifier as in \MSSQL.1\MSSQL\Data.  <b>Note:</b> Clicking Default displays the correct installation directory, if you entered the database server and instance name correctly. If you click Default and the correct installation directory does not appear, your database creation fails.
Admin User Name	admin	Name of the default user name that is used to log on to the Symantec Endpoint Protection Manager Console for the first time.  (not changeable)
Admin Password	None	The password specified during server configuration to use with the admin user name.

## Installing Symantec Endpoint Protection Manager with a SQL Server database

You can install the Symantec Endpoint Protection Manager on the same computer that runs Microsoft SQL Server and then create a database on the local SQL server. You can also install the Symantec Endpoint Protection Manager on a computer that does not run SQL Server and then create a database on a remote computer running SQL Server. In either scenario, make sure that the appropriate SQL Server components are properly configured on each computer.

See [“SQL Server requirements for installing Symantec Endpoint Protection Manager”](#) on page 35.

---

**Note:** If you create a new database, SQL Server automatically manages your database with the simple recovery model and enables Auto Shrink.

---

### To install the Symantec Endpoint Protection Manager

- 1 Insert the installation CD, and start the installation.
- 2 In the Welcome panel, do one of the following:
  - To install for Symantec Endpoint Protection, click **Install Symantec Endpoint Protection Manager**.
  - To install for Symantec Network Access Control, click **Install Symantec Network Access Control**, and then click **Install Symantec Endpoint Protection Manager**.
- 3 Click through the panels, until the Destination Folder panel appears.
- 4 In the Destination Folder panel, accept or change the default installation directory.
- 5 Do one of the following:
  - To let the Symantec Endpoint Protection Manager IIS Web server run with other Web sites on this computer, check **Use the default Web site**, and then click **Next**.
  - To configure the Symantec Endpoint Protection Manager IIS Web as the only Web server on this computer, check **Create a custom Web site**, and then click **Next**.
- 6 On the Ready to Install the Program panel, click **Install**.
- 7 When the installation finishes and the Installation Wizard Complete panel appears, click **Finish**.

The Server Configuration Wizard panel can take up to 15 seconds to appear. If you are prompted to restart the computer, restart the computer. When you log on, the Server Configuration Wizard panel appears automatically.

### To create an SQL database

- 1 In the Management Server Configuration Wizard panel, select **Advanced**, and then click **Next**.
- 2 Select the number of clients that you want the server to manage, and then click **Next**.
- 3 Check **Install my first site**, and then click **Next**.
- 4 In the Server Information panel, accept or change the default values for the following boxes, and then click **Next**:

- Server name
  - Server port
  - Web console port
  - Server data folder
- 5 In the Site Information panel, in the Site name box, accept or change the default name, and then click **Next**.
  - 6 In the Create Encryption Password panel, in the Create encryption password boxes, type a password, and then click **Next**.

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

- 7 In the Database type selection panel, check **Microsoft SQL Server**, and then click **Next**.
- 8 In the Define New Database panel, do one of the following:
  - If the database does not exist, check **Create a new database** (recommended).
  - If the database does exist, check **Use an existing database**.

An existing database must define file groups PRIMARY, FG\_CONTENT, FG\_LOGININFO, FG\_RPTINFO, and FG\_INDEX. The user account for database access must have privileges db\_ddladmin, db\_datareader, and db\_datawriter. If these requirements are not met, your installation fails. A best practice is to define a new database.

- 9 Click **Next**.
- 10 In the Microsoft SQL Server Information panel, type your values for the following boxes, and then click **Next**:
  - Database server  
If you created a new instance, the format is *servername\_or\_IPaddress\instance\_name*.
  - SQL server port
  - Database name
  - User
  - Password
  - Confirm password (only when creating a new database)

- SQL Client folder
  - DBA user (only when creating a new database)
  - DBA password (only when creating a new database)
  - Database data folder
- 11 Specify and confirm a password for the Symantec Endpoint Protection Manager admin account. Optionally, provide an administrator email address.
  - 12 Click **Next**.
  - 13 In the Warning dialog prompt, read and understand the warning information about clear text communications, and then click **OK**.
  - 14 In the Configuration Completed panel, do one of the following:
    - To deploy client software with the Migration and Deployment Wizard, click **Yes**.
    - To log on to the Symantec Endpoint Protection Manager Console first, and then deploy client software, click **No**.

Refer to the Client Installation chapter for details on how to deploy client software.

After you install Symantec Endpoint Protection Manager and become comfortable with administration tasks, you should secure your cryptographic files in case you need to recover from a disaster. You should also document your encryption password that you enter during Symantec Endpoint Protection Manager installation.

## Logging on to the Symantec Endpoint Protection Manager Console

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

### To log on to the Symantec Endpoint Protection Manager Console

- 1 Click **Start > Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Console**.
- 2 In the Symantec Endpoint Protection Manager logon prompt, in the User name box, type **admin**.
- 3 In the Password box, type the admin password that you created during installation, and then click **Log On**.

# Configuring your product after installation

This chapter includes the following topics:

- [Setting up the organizational structure and updating content](#)
- [Adding a group](#)
- [About importing the organizational structure](#)
- [Adding clients as users or as computers](#)
- [Adding a location with a wizard](#)
- [Adding an administrator account](#)
- [About LiveUpdate Policies](#)
- [Configuring a LiveUpdate Settings Policy](#)
- [Configuring a LiveUpdate Content Policy](#)

## Setting up the organizational structure and updating content

After you install the management server, you set up the organizational structure. You can also configure a LiveUpdate Policy to download the latest signatures and other content to the client computers.

**Table 3-1** Process after installing the Symantec Endpoint Protection Manager

To perform this step	Description	See this section
Step 1	Add a group. You can add new groups or import your existing organizational structure.	See <a href="#">“Adding a group”</a> on page 44. See <a href="#">“About importing the organizational structure”</a> on page 45.
Step 2	Add a client as either a user or a computer.	See <a href="#">“Adding clients as users or as computers”</a> on page 45.
Step 3	Add a location.	See <a href="#">“Adding a location with a wizard”</a> on page 46.
Step 4	Add an administrator account.	See <a href="#">“Adding an administrator account”</a> on page 48.
Step 5	Update the content on the clients. You can set up a LiveUpdate Content Policy and a LiveUpdate Settings Policy.	See <a href="#">“About LiveUpdate Policies”</a> on page 49.

## Adding a group

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

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

---

**Note:** You cannot add groups to the Temporary group.

---

### To add a group

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

## About importing the organizational structure

You can import group structures, or organizational units. To import the organizational units, you use an LDAP directory server or an Active Directory server. 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 organizational unit. You can assign security policies to the imported organizational unit. 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 it was imported has priority. A user account can exist in both the organizational unit and in an outside group. The policy that was applied to the outside group has priority in this scenario.

You can import and synchronize information about user accounts and computer accounts from an Active Directory server or an LDAP server.

## Adding clients as users or as computers

All clients must be assigned to a group. Groups should contain clients with the same security needs and settings.

You can manually add users to a group. In most cases, however, this procedure is not practical unless you want to add a limited number of users for maintenance purposes. Most administrators import user lists from an LDAP server or a Domain server.

See [“About importing the organizational structure”](#) on page 45.

You can first manually add a user to a specific group and later install the client with a preferred group assigned to it. You do this task by associating group policies during package creation. The client gets added to the group that is specified on the server rather than the group that is specified in the package.

You can add a client as a computer to any group. The primary reason to add a client as a computer is to protect the computer regardless of who logs on to it. For example, a computer may be located in a vulnerable or unsecured location such as a public lobby. You can add this computer to a group that contains other public computers and assign very stringent security policies to the group.

Be aware of the following facts when you add computers to groups:

- You can add a computer to more than one group.
- You must know the actual computer name and the domain before you can add a computer.

- The maximum length of the computer name is 64 characters.
- The maximum length of the description field is 256 characters.

Make sure that clients are not blocked from being added to the groups.

#### To add clients as users

- 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, click **Add User Account**.
- 4 In Add User for *group name* dialog box, in the User Name text box, type the name of the new user.
- 5 Under Domain Name, choose whether to log on to a specified domain or to log on to the local computer.
- 6 In the Description text box, type an optional description of the user.
- 7 Click **OK**.

#### To add clients as computers

- 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, click **Add Computer Account**.
- 4 In the Add Computer dialog box, type the name of the computer and the domain that you want the computer to be added to.
- 5 In the Description text box, optionally type a short description of the computer.
- 6 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.

**To add a location with a wizard**

- 1 In the Symantec Endpoint Protection Manager 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
  - Avenail SSL VPN
  - Juniper SSL VPN

- 8 Click **Next**.
- 9 In the Add Location Wizard Complete panel, click **Finish**.

## 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.

---

**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 On the Symantec Endpoint Protection Manager console, click **Admin**.
- 2 On the Admin page, under Tasks, click **Administrators**, and then click **Add Administrator**.

- 3 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.
- 4 Optionally enter the full name of the administrator in the second text box.
- 5 Type and retype the password.  
The password must be six or more characters. All characters are permitted.
- 6 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.
- 7 Click **OK**.
- 8 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, and then configure the rights for a limited administrator.
- 9 Click **OK**.

## 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.

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.

## 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 4 hours. You should also know the place from which you want your client computers to check for and get updates. Generally, 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:** An advanced setting is available to let users manually start LiveUpdate from their client computers and the setting is disabled by default. If you enable this setting, users can start LiveUpdate and download the latest content virus definitions, component updates, and potential product updates. If the advanced policy setting for Download product updates using LiveUpdate is enabled, the product updates that they download are maintenance releases and patches for Symantec client software. 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. A best practice is to leave this setting disabled.

---

### To configure a LiveUpdate Settings Policy

- 1 In the console, click **Policies**.
- 2 In the View Policies pane, click **LiveUpdate**.
- 3 On the LiveUpdate Settings tab, in the Tasks pane, click **Add a LiveUpdate Settings Policy**.
- 4 In the Overview pane, in the Policy name box, type a name for the policy.
- 5 Under LiveUpdate Policy, click **Server Settings**.
- 6 In the Server Settings pane, under Internal or External LiveUpdate Server, check and enable at least one source from which to retrieve updates.  
  
Most organizations should use the default management server.
- 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 Computers and Users Policies tab.

## Configuring a LiveUpdate Content Policy

By default, all Symantec Endpoint Protection clients in a group receive the latest versions of all content and 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. If the LiveUpdate Content Policy allows all updates, but the management server is not configured to download all updates, the clients receive only what the server downloads.

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 for an update, the clients never receive updates for this particular update until the setting is changed from a specific revision to the latest available. LiveUpdate servers do not understand named version functionality.

Named versions let you exercise tighter control over the updates that get distributed to clients. Typically, the environments that test the latest updates before distributing them to clients use named version functionality.

---

**Note:** Using specific revisions provides rollback functionality.

---

### To configure a LiveUpdate Content Policy

- 1** In the console, click **Policies**.
- 2** In the View Policies pane, click **LiveUpdate**.
- 3** On the LiveUpdate Content tab, click **Add a LiveUpdate Content Policy**.

- 4 In the Overview pane, in the Policy name box, type a name for the policy.
- 5 In the LiveUpdate Content pane, click **Security Definitions**.
- 6 In the Security definitions pane, check the updates to download and install, and uncheck the updates to disallow.
- 7 For each update, do one of the following actions:
  - Check **Use latest available**
  - Check **Select a revision**
- 8 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 [11](#).
  - If you did check Select a revision for an update type, click **Edit**, and then continue with the next step.
- 9 In the Select Revision dialog box, in the Revision column, select the revision to use, and then click **OK**.
- 10 In the LiveUpdate Content window, click **OK**.
- 11 In the Assign Policy dialog box, click **Yes**.

You can optionally cancel out of this procedure, and assign the policy at a later time.
- 12 In the Assign LiveUpdate Content Policy dialog box, check one or more groups to which to assign this policy, and then click **Assign**.

# Creating policies

This chapter includes the following topics:

- [About policies](#)
- [Evaluating policies](#)
- [Setting up and testing an Antivirus and Antispyware Policy](#)
- [Setting up and testing a Firewall Policy](#)
- [Setting up and testing a custom IPS library](#)
- [Setting up and testing an Application and Device Control Policy](#)

## About policies

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 them to suit your specific environment.

[Table 4-1](#) lists the different types of policies. It also includes whether or not a default policy is created during the initial installation, and a description of each type of policy.

**Table 4-1** Symantec Endpoint Protection Manager policies

Policy name	Default policy	Description
Antivirus and Antispyware	Yes	Defines the antivirus and antispyware threat scan settings, including how detected processes are handled.

**Table 4-1** Symantec Endpoint Protection Manager policies (*continued*)

Policy name	Default policy	Description
Firewall	Yes	Defines the firewall rules that allow and block traffic, and specifies settings for smart traffic filtering, traffic, and peer-to-peer authentication.
Intrusion Prevention	Yes	Defines the exceptions to the intrusion prevention signatures and specifies intrusion prevention settings, such as active response.
Host Integrity	Yes	Helps define, restore, and enforce the security of clients to keep enterprise networks and data secure.
Application and Device Control	Yes	Protects system resources from applications and manages the peripheral devices that can attach to computers.
LiveUpdate	Yes	Specifies the computers that clients must contact to check for updates along with the schedule which defines how often clients must check for updates.
Centralized Exceptions	No	Specifies the exceptions to the particular policy features that you want to apply.

You can perform the following tasks on all policies:

- Add  
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.
- Edit
- Delete
- Assign
- Replace
- Copy and paste

■ Import and export

You can withdraw any type of policy except an Antivirus and Antispyware Policy and a LiveUpdate Settings Policy.

## Evaluating policies

[Table 4-2](#) lists the main policy types you should evaluate after you first install the management server.

**Table 4-2** Process for evaluating policies

To perform this step	Description	See this section
Step 1	Create and test an Antivirus and Antispyware Policy.  You can define the antivirus and antispyware threat scan settings, including how detected processes are handled.	See <a href="#">“Setting up and testing an Antivirus and Antispyware Policy”</a> on page 59.
Step 2	Create and test a Firewall Policy.  You can define the firewall rules that allow and block traffic, and specify settings for smart traffic filtering, traffic, and peer-to-peer authentication.	See <a href="#">“Setting up and testing a Firewall Policy”</a> on page 76.
Step 3	Create and test an Application and Device Control Policy.  You can protect the system resources from applications and manage the peripheral devices that can attach to computers.	See <a href="#">“Setting up and testing an Application and Device Control Policy”</a> on page 89.
Step 4	Create and test a custom intrusion prevention system (IPS) library.  You can create packet-based signatures that detect attacks in the TCP/IP stack. Packet-based signatures examine a single packet that matches a rule.	See <a href="#">“Setting up and testing a custom IPS library”</a> on page 80.

**Table 4-2** Process for evaluating policies (*continued*)

To perform this step	Description	See this section
Step 5	Create and test a Host Integrity Policy.  You can evaluate whether a computer is properly protected and compliant before allowing it to connect to the corporate network.	See <a href="#">“Setting up and testing a Host Integrity Policy”</a> on page 111.

To evaluate a policy, you create a policy and then test it on the client computer.

**Table 4-3** Process for creating and testing policies

To perform this step	Description	See this section
Step 1	Add a new policy. All new policies include the default settings.	See <a href="#">“Adding a shared policy”</a> on page 56.
Step 2	Once you have completed the configuration of the policy, assign the policy to a group or location.	See <a href="#">“Assigning a shared policy”</a> on page 57.
Step 3	To test the policy, on the client computer, check that the client has the updated policy. You can also manually update the policy.	See <a href="#">“Updating the policy file manually”</a> on page 58.  See <a href="#">“Verifying that policies have been updated”</a> on page 58.

## 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.

### 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 57.

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**.

## 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.

### To assign a shared policy

- 1 Create a shared policy.  
See [“Adding a shared policy”](#) on page 56.
- 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.

## Updating the policy file manually

The settings that control protection on the client are stored on the computer in a policy file. The policy file updates the settings for Antivirus and Antispyware Protection, Network Threat Protection, Proactive Threat Protection, and Network Access Control. This policy file normally updates automatically. However, you can also update the policy file manually if you do not want to wait until the policy file is updated.

---

**Note:** You can view the System log to verify that the operation updated the policy successfully.

---

### To update the policy file manually

- 1 In the Windows notification area, right-click the client icon.
- 2 In the pop-up menu, click **Update Policy**.

## Verifying that policies have been updated

When you change or assign a policy, check to see that your clients receive the updated policy.

### To verify that a policy updated from the Symantec Endpoint Protection Manager

- 1 On the console, click **Monitors**, and then click **Logs**.
- 2 In the Log Type list, click **System**.
- 3 In the Log content list, click **Client-Server Activity**.
- 4 Click **View Log**.

You see an entry for a policy download for each client.

**To verify that the client computers obtained updated policies**

- 1 On the client computer, in the main Symantec Endpoint Protection window, click **View Logs**.
- 2 Beside Client Management, click **View Logs**, and then click **System Log**.  
 You see an entry for the policy update that contains the serial number.

# Setting up and testing an Antivirus and Antispyware Policy

You can implement antivirus and antispyware technology on your network by using a Symantec Endpoint Protection Antivirus and Antispyware Policy.

Although TruScan proactive threat scans are configured as part of your Antivirus and Antispyware Policy, they are beyond the scope of this discussion. Some background information is provided.

**Table 4-4** Process to set up and test an Antivirus and Antispyware Policy

To perform this step	Description	See this section
Step 1	Decide which of the default antivirus and antispyware policies you want to base your antivirus and antispyware security on.	See <a href="#">“About the preconfigured Antivirus and Antispyware Policies”</a> on page 61.
Step 2	Configure a scheduled scan and add it to the default Antivirus and Antispyware Policy you selected.	See <a href="#">“Adding scheduled scans to an Antivirus and Antispyware Policy”</a> on page 62.
Step 3	Change the action for a security risk in the default Antivirus and Antispyware Policy you selected.	See <a href="#">“Configuring actions for known virus and security risk detections”</a> on page 63.
Step 4	Configure a user notification for client computers in the default Antivirus and Antispyware Policy you selected.	See <a href="#">“About notification messages on infected computers”</a> on page 64. See <a href="#">“Customizing and displaying notifications on infected computers”</a> on page 65.
Step 5	Assign the policy to a group.	See <a href="#">“Assigning a shared policy”</a> on page 57.
Step 6	Check to see that the policy is updated on the clients.	See <a href="#">“Verifying that policies have been updated”</a> on page 58.

**Table 4-4** Process to set up and test an Antivirus and Antispyware Policy  
(continued)

To perform this step	Description	See this section
Step 7	Test to see that the Antivirus and Antispyware Policy works.	See <a href="#">“Testing to see that the Antivirus and Antispyware Policy works”</a> on page 67.
Step 8	Read about TruScan Proactive Threat scanning.	<p>See <a href="#">“About TruScan proactive threat scans”</a> on page 67.</p> <p>See <a href="#">“About using the Symantec default settings”</a> on page 68.</p> <p>See <a href="#">“About the processes that TruScan proactive threat scans detect”</a> on page 69.</p> <p>See <a href="#">“About managing false positives detected by TruScan proactive threat scans”</a> on page 70.</p> <p>See <a href="#">“About the processes that TruScan proactive threat scans ignore”</a> on page 72.</p> <p>See <a href="#">“Understanding TruScan proactive threat detections”</a> on page 73.</p>

## 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.

---

## 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.

## Adding scheduled scans to an Antivirus and Antispyware Policy

You configure scheduled scans as part of an Antivirus and Antispyware Policy.

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 add a scheduled scan to an Antivirus and Antispyware Policy

- 1 On the Antivirus and Antispyware Policy page, 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 which directories to scan.
- 8 Under File types, click **Scan all files** or **Scan only selected extensions**.
- 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 page 63.  
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 64.
- 16 If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.
- 17 Click **OK**.

#### To add a scheduled scan from a template

- 1 On the Antivirus and Antispyware Policy page, 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 scheduled scan from a Scheduled Scan Template**.
- 4 Select the scan template that you want to use for this policy.
- 5 Click **OK**.

## Configuring actions for known virus and security risk detections

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 67.

Actions allow you to set how the client software responds when it detects a known virus or a security risk. 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 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

- 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 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 If you are finished with the configuration for 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.

**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 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:

- Add warnings to infected email message
- Notify senders of infected email messages
- Notify users of infected email messages.

Notifications for proactive threat scan results are configured separately.

## 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 4-5](#) describes the variable fields that are available for notifications.

**Table 4-5** Notification message variables

Field	Description
SecurityRiskName	The name of the virus or security risk that was found.

**Table 4-5** Notification message variables (*continued*)

Field	Description
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.
Status	The state of the file: Infected, Not Infected, or Deleted.  This message variable is not used by default. To display this information, you must manually add this variable to the message.
Filename	The name of the file that the virus or the security risk has infected.
PathAndFilename	The complete path and name of the file that the virus or the security risk has infected.
Location	The drive on the computer on which the virus or security risk was located.
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.
Event	The type of event, such as Risk Found.
LoggedBy	The type of scan that detected the virus or security risk.
DateFound	The date on which the virus or security risk was found.
StorageName	The affected area of the application (for example, File System Auto-Protect or Lotus Notes Auto-Protect).
ActionDescription	A full description of the actions that were taken in response to the detection of the virus or the security risk.

### To display notification messages on infected computers

- 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**.

## Testing to see that the Antivirus and Antispyware Policy works

To test to see that the Antivirus and Antispyware Policy works you can use the test virus file eicar.com. The EICAR test virus is a text file that the European Institute for Computer Anti-Virus Research (EICAR) developed. It provides an easy way and safe way to test most antivirus software. You can use it to verify that the antivirus portion of the client works.

**To test the Antivirus and Antispyware Policy**

- 1 On the client computer, download the antivirus test file from the EICAR Web site.

This file is available from the following URL: [www.eicar.org](http://www.eicar.org)

- 2 Download and run the eicar.com test file.  
A notification appears that tells you that a risk is found.
- 3 In the Symantec Endpoint Protection Manager console, on the Monitors page, click **Logs**.
- 4 On the Logs tab, in the Log type drop-down list, click **Risk**, and then click **View Log**.

On the Risk Logs page, the Virus found event appears.

## 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.

---

**Note:** TruScan proactive threat scans is another name for proactive threat scanning, and may appear in the user interface. The meaning is the same.

---

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.

---

**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 73.

See [“Specifying the actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers”](#) on page 75.

## 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.

[Table 4-6](#) describes the processes that proactive threat scans detect.

**Table 4-6** Processes detected by TruScan proactive threat scans

Type of processes	Description
Trojan horses and worms	<p>Processes that exhibit the characteristics of Trojan horses or worms.</p> <p>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.</p>
Keyloggers	<p>Processes that exhibit the characteristics of keyloggers.</p> <p>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.</p>
Commercial applications	<p>Known commercial applications that might be used for malicious purposes.</p> <p>Proactive threat scans detect several different types of commercial applications. You can configure actions for two types: keyloggers and remote control programs.</p>
Adware and spyware	<p>Processes that exhibit the characteristics of adware and spyware</p> <p>Proactive threat scans uses heuristics to detect the unknown processes that behave like adware and spyware. These processes may or may not be risks.</p>

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.

## 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.

[Table 4-7](#) outlines the tasks for creating a plan to manage false positives.

**Table 4-7** Plan for managing false positives

Task	Description
Ensure that Symantec manages Trojan horse, worm, and keylogger detections.	<p>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.</p> <p>When Symantec manages the detections, proactive threat scans perform an action that is based on how the scan interprets the detection.</p> <p>The scan applies one of the following actions to the detection:</p> <ul style="list-style-type: none"> <li>■ <b>Quarantine</b> The scan uses this action for the detections that are likely to be true threats.</li> <li>■ <b>Log only</b> The scan uses this action for the detections that are likely to be false positives.</li> </ul> <p><b>Note:</b> 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.</p>

**Table 4-7** Plan for managing false positives (*continued*)

Task	Description
<p>Ensure that Symantec content is current.</p>	<p>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.</p> <p>You can run a report in the console to check which computers are running the latest version of the content.</p> <p>You can update the content by doing any of the following actions:</p> <ul style="list-style-type: none"> <li>■ Apply a LiveUpdate Policy. See “<a href="#">About LiveUpdate Policies</a>” on page 49.</li> <li>■ Run the Update command for the selected computers that are listed on the Clients tab.</li> <li>■ Run the Update command on the selected computers that are listed in the computer status or risk log</li> </ul>
<p>Make sure that submissions are enabled.</p>	<p>Submissions settings are included as part of the Antivirus and Antispyware Policy.</p> <p>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.</p>
<p>Create exceptions for the false positives that you discover.</p>	<p>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.</p>

## 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.

## 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.

---

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. 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.

---

**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.

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.

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.

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**.

## Setting up and testing a Firewall Policy

You can configure the firewall on client computers by using a Firewall Policy.

A Firewall Policy offers the following types of protection for client computers:

- Firewall rules control how the firewall protects computers from malicious incoming traffic and applications. The firewall automatically checks all the incoming packets and outgoing packets against these rules. The firewall allows or blocks the packets that are based on the information that is specified in the rules.
- Smart traffic filters allow DHCP, DNS, and WINS traffic.
- Traffic and stealth settings detect and block the traffic that comes from certain drivers, protocols, and other sources.

- Peer-to-peer authentication blocks a remote computer from connecting to a client computer until the client computer has authenticated that remote computer. Peer-to-peer authentication works with the Host Integrity Policy.

**Table 4-8** Process for setting up and testing a Firewall Policy

To perform this step	Description	See this section
Step 1	Create a Firewall Policy to allow or block an application.	See <a href="#">“Creating a Firewall Policy to allow or block an application”</a> on page 78.
Step 2	Assign the policy to a group.	See <a href="#">“Assigning a shared policy”</a> on page 57.
Step 3	Check that the policy is updated on the clients.	See <a href="#">“Verifying that policies have been updated”</a> on page 58.
Step 4	Test to see that the Firewall Policy works.	See <a href="#">“Testing the Firewall Policy”</a> on page 79.

## 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.

### 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.

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.

## Creating a Firewall Policy to allow or block an application

You can create a rule in a Firewall Policy to allow or block a specific application on a client computer. For example, you can choose to allow or block Internet Explorer from connecting to resources outside the firewall by adding a rule to a Firewall Policy. You can also create rules to allow or block specific types of traffic, host communications, or network services.

When you create a rule, it is by default set to allow the application specified. You can change the rule to block the application after it is created.

---

**Note:** To test the rule that is created in this procedure, Internet Explorer must be installed on the client computer.

---

### To create a Firewall Policy to allow or block an application

- 1 In the console, click **Policies**.
- 2 On the Policies page, under View Policies, click **Firewall**.
- 3 Under Tasks, click **Add a Firewall Policy**.
- 4 Specify a name and optional description for the policy.
- 5 Confirm that **Enable this policy** is selected.
- 6 On the Firewall Policy page, click **Rules**.

- 7 On the Rules tab, under the Rules list, click **Add Rule**.
- 8 In the Add Firewall Rule Wizard, click **Next**.
- 9 In the Select Rule Type panel, select **Application**, and then click **Next**.
- 10 On the Specify Application Information panel, select **Define an application**, and then click **Next**.
- 11 On the Define an Application panel, in the File Name field, type **iexplore.exe**.  
You can also browse to the file, or type the full path to the file in the field.
- 12 Optionally, enter values for the File Description, Size, Last Modified, and File Fingerprint fields.
- 13 Click **Next**.
- 14 Click **Finish** to close the wizard.
- 15 To configure the rule to block Internet Explorer, select the rule that lists iexplorer.exe in the Application column.  
It should be the last row above the blue line in the table.
- 16 Right-click **Allow** in the Action column, and then select **Block**.
- 17 On the Rules page, click **OK**.
- 18 Assign the policy to a group.  
See “[Assigning a shared policy](#)” on page 57.

## Testing the Firewall Policy

You can test the updated Firewall Policy on the client computer by opening Internet Explorer and attempting to access the Symantec Web site at <http://www.symantec.com>. You must use a client computer from which you are able to connect to Internet Web sites. If the rule to block Internet Explorer was successfully updated on the client, the browser tries to access the page for several seconds, and then displays a message indicating that the Web page or server cannot be found.

You can confirm that it is the rule blocking the communication by turning off Network Threat Protection on the client. When the protection is turned off, open a new Internet Explorer window and try to access the Symantec Web site. When the Web site is loaded, turn on Network Threat Protection, and then try to refresh the Web page. After several seconds, the browser again displays a message indicating the page or server could not be found.

# Setting up and testing a custom IPS library

A custom IPS library is a collection of custom IPS signatures. You can create custom IPS signatures to supplement or replace the Symantec IPS signatures in the Intrusion Prevention Policy.

**Table 4-9** Process for setting up and testing a custom IPS library

To perform this step	Description	See this section
Step 1	Read about custom IPS signatures and how to write the signature syntax for sample custom IPS signatures. The two signatures detect attempts to download MP3 files through a Web browser and FTP.	See <a href="#">“About custom IPS signatures”</a> on page 80. See <a href="#">“About creating custom IPS signatures to detect an attempt to download MP3 files”</a> on page 82.
Step 2	Create the custom IPS library and add a custom IPS signature.	See <a href="#">“Creating custom IPS signatures”</a> on page 84.
Step 3	Assign the policy to a group.	See <a href="#">“Assigning a shared policy”</a> on page 57. See <a href="#">“Assigning multiple custom IPS libraries to a group”</a> on page 87.
Step 4	Check to see that the policy is updated on the clients.	See <a href="#">“Verifying that policies have been updated”</a> on page 58.
Step 5	Test to see that the custom IPS signature works.	See <a href="#">“Testing the custom IPS signature”</a> on page 88.

## 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.

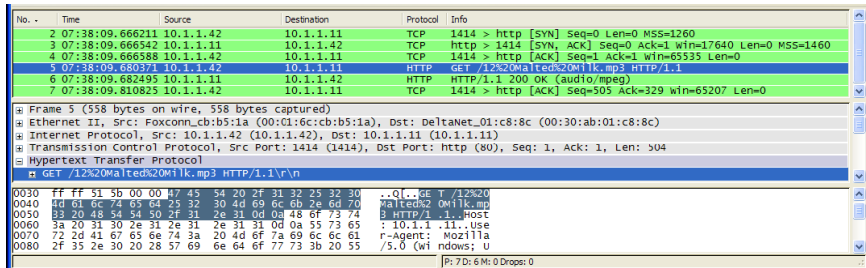
See “Creating custom IPS signatures” on page 84.

## About creating custom IPS signatures to detect an attempt to download MP3 files

You can create sample custom IPS signatures to detect an attempt to access and download MP3 files through a Web browser or FTP. To detect an MP3 file and then block access to it, you write two signatures. One signature detects an MP3 file through the HTTP service. The second signature detects an MP3 files through the FTP service.

The format of an MP3 file makes it difficult to detect an MP3 file in network traffic. However, you can view the TCP packets to find the commands and protocols that are used to retrieve the MP3 files. You can then use this information to create the syntax for a custom IPS signature.

The following figure displays a packet capture of an HTTP GET request for an MP3 file:



During an HTTP or FTP session, the server and the client exchange information. The information is contained in the TCP packets that are destined for the appropriate service on the server. The HTTP service uses port 80 and the FTP service uses port 21. The TCP packets contain the required information in a payload component.

The highlighted packets show the HTTP GET command that a Web browser uses when it download files. The FTP client uses the FTP RETR command to download files. The FTP command is also used when multiple files are retrieved by using the MGET command. The file name and respective mp3 extension is present in both requests. Both protocols insert [CR][LF] characters to mark the end of the request.

The custom signatures must also contain several parameters, including a regular expression that identifies the specific commands that should be blocked. Regular expressions are patterns of the characters that are compared against the contents of the packet. The commands you want to block are contained in these packets. Because you would not know the file name of the MP3 file, you can use the wildcard character (\*) to match the unknown number of characters between the command and the file name. The command must be in lower case, but the file extension can be in either case.

Use the standard syntax to write the content for the content:

```
rule protocol-type, [protocol-options,] [ip-protocol
option,] msg, content...
```

The content of the HTTP signature contains the following syntax:

```
rule tcp, dest=(80,443), tcp_flag&ack, saddr=$LOCALHOST,
msg="MP3 GET in HTTP detected",
regexcontent="[Gg][Ee][Tt] .*[Mm][Pp]3 .*\x0d\x0a"
```

The content of the FTP signature contains the following syntax:

```
rule tcp, dest=(21), tcp_flag&ack, saddr=$LOCALHOST,
msg="MP3 GET in FTP detected",
regexcontent="[Rr][Ee][Tt][Rr] .*[Mm][Pp]3\x0d\x0a"
```

**Table 4-10** breaks down the pieces of the HTTP signature and the FTP signature.

**Table 4-10** HTTP signature and FTP signature syntax

Use the following syntax	To perform the following task
For the HTTP signature: <pre>rule tcp dest=(80,443)</pre> For the FTP signature: <pre>rule tcp dest=(21)</pre>	Tells the packet-based engine what traffic to search. This way, the engine does not search unnecessary traffic and does not use up system resources. The more detailed information your provide, the better the packet-based engine performs.  This argument limits the destination ports to 80 and 443 for the HTTP service and to 21 for the FTP service.
<pre>tcp_flag&amp;ack</pre>	Reduces the false positives.
<pre>saddr=\$LOCALHOST</pre>	Makes sure that the request originates on the host.

**Table 4-10** HTTP signature and FTP signature syntax (*continued*)

Use the following syntax	To perform the following task
<p>For the HTTP signature:</p> <pre>msg="MP3 GET in HTTP"</pre> <p>For the FTP signature:</p> <pre>msg="MP3 GET in FTP"</pre>	<p>Displays the name for the signature when the signature is triggered. The name appears in the Security Log. Use a descriptive string so that you can identify the triggered signature in the log.</p>
<p>For the HTTP signature:</p> <pre>regexcontent="[Gg][Ee][Tt].*[Mm][Pp]3.*\x0d\x0a"</pre> <p>For the FTP signature:</p> <pre>regexcontent="[Rr][Ee][Tt][Rr].*[Mm][Pp]3\x0d\x0a"</pre>	<p>Matches this string in the HTTP traffic or the FTP traffic with the payload in the TCP packets. To reduce false positives, use this argument carefully.</p> <p>The string matches the ASCII text of the TCP packet, which is "GET [.*].mp3[CR][LF]" for the HTTP signature and "RETR [.*].mp3[CR][LF]" for the FTP signature.</p> <p>The string is written so that the text can be case-insensitive.</p>

## 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.

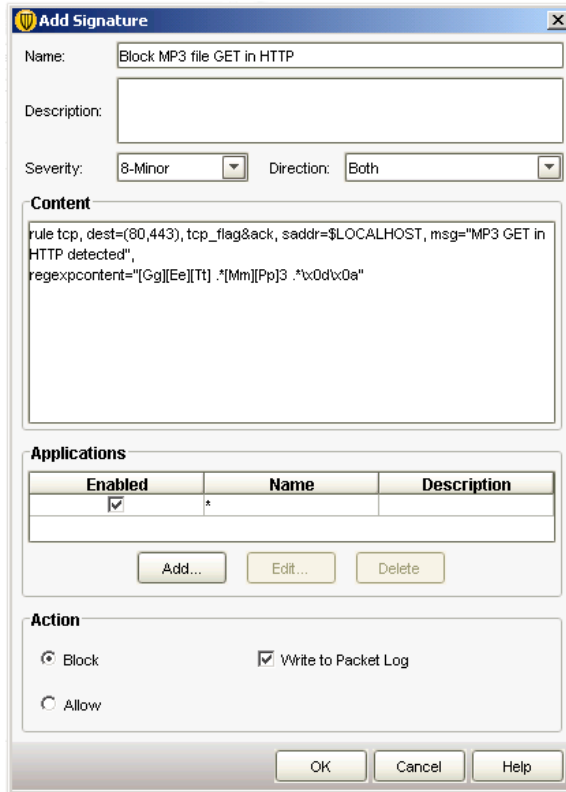
**To add a custom signature**

- 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 example, the HTTP signature includes the following syntax:

```
rule tcp, dest=(80,443), tcp_flag&ack, saddr=$LOCALHOST,  
msg="MP3 GET in HTTP detected",  
regexcontent="[Gg][Ee][Tt] .*[Mm][Pp]3 .*\x0d\x0a"
```



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 Microsoft Internet Explorer, type the file name as **ieexplore** or **ieexplore.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.**

For example, the FTP signature includes the following syntax:

```
rule tcp, dest=(21), tcp_flag&ack, saddr=$LOCALHOST,
msg="MP3 GET in FTP detected",
regexpcontent="[Rr][Ee][Tt][Rr] .*[Mm][Pp]3\x0d\x0a"
```

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 57.

You can also assign multiple custom IPS libraries to a group.

See [“Assigning multiple custom IPS libraries to a group”](#) on page 87.

## 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**.

## Testing the custom IPS signature

To test the custom IPS signatures, you can perform the following tasks, in this order:

- Check to be sure that the policy was updated on the client computer.  
The next time that the client receives the policy, the client applies the new IPS signatures.  
See [“Verifying that policies have been updated”](#) on page 58.
- Try to download an MP3 file on to the client computer.  
To test both signatures, you try to download an MP3 file through both an FTP client and a Web browser. If the download does not occur or times out after many attempts, the custom IPS signature is successful.
- View the blocked events on the Symantec Endpoint Protection Manager Console.  
You can view the events that the Network Threat Protection Attacks log recorded after the client blocked the MP3 file from being downloaded.

### To try to download the MP3 file on to the client computer

- 1 On the client computer, try to download an MP3 file to an FTP client.  
The client can be command-line-based or GUI-based, because all the tested clients use the same RETR command. The command times out, and the remote server resets the connection, which disconnects the client.
- 2 Open a Web browser such as Internet Explorer, and try to download an MP3 file.  
The download should not occur.  
The client records these events in the Security Log and Packet Log. The client then sends the results to the management server within a couple of minutes.

**To view the blocked event in the Symantec Endpoint Protection Manager Console**

- 1 In the Console, click **Monitors**, and then click **Logs**.
- 2 On the Logs tab, in the Log type drop-down list, click **Network Threat Protection**.
- 3 In the Log content drop-down list, click **Attacks**, and then click **View Logs**.
- 4 In the Network Threat Protection Logs pane, click **MP3 GET in HTTP detected** or **MP3 GET in FTP detected**, and then click **Details**.
- 5 Close the Detailed Network Threat Protection Event Information dialog box.

## Setting up and testing an Application and Device Control Policy

You can implement application and device control on client computers by using an Application and Device Control Policy.

An Application and Device Control Policy offers the following types of protection for client computers:

- Application control monitors the Windows API calls made on client computers and controls access to clients' files, folders, registry keys, and processes. It protects system resources from applications.
- Device control manages the peripheral devices that can attach to computers.

**Table 4-11** Process for setting up and testing an Application and Device Control Policy

To perform this step	Description	See this section
Step 1	Enable the rule sets that you want to use in the default Application and Device Control Policy.	See <a href="#">“Enabling a default application control rule set”</a> on page 90.
Step 2	Create a new application control rule set and add it to the default Application and Device Control Policy.	See <a href="#">“Creating a new application control rule set and adding a new rule to the set”</a> on page 91.

**Table 4-11** Process for setting up and testing an Application and Device Control Policy (*continued*)

To perform this step	Description	See this section
Step 3	<p>Read about device control.</p> <p>Add a hardware device to the Hardware Devices list.</p> <p>Customize the device control part of the default Application and Device Control Policy.</p>	<p>See <a href="#">“About device control”</a> on page 99.</p> <p>See <a href="#">“Adding a hardware device to the Hardware Devices list”</a> on page 101.</p> <p>See <a href="#">“Configuring device control for an Application and Device Control Policy”</a> on page 102.</p>
Step 4	Assign the policy to a group.	See <a href="#">“Assigning a shared policy”</a> on page 57.
Step 5	Check to see that the policy is updated on the clients.	See <a href="#">“Verifying that policies have been updated”</a> on page 58.

## 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.

### 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.

For example, next to the Block writing to USB drives rule set, check the check box in the Enabled column.

- 9 Click **OK**.

#### To test the Block writing to USB drives rule set

- 1 On the client computer, attach a USB drive.
- 2 Open Windows Explorer and double-click the USB drive.
- 3 Right-click the window and click **New > Folder**.
- 4 If application control is in effect, an **Unable to create folder** error message appears.

## 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, 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.

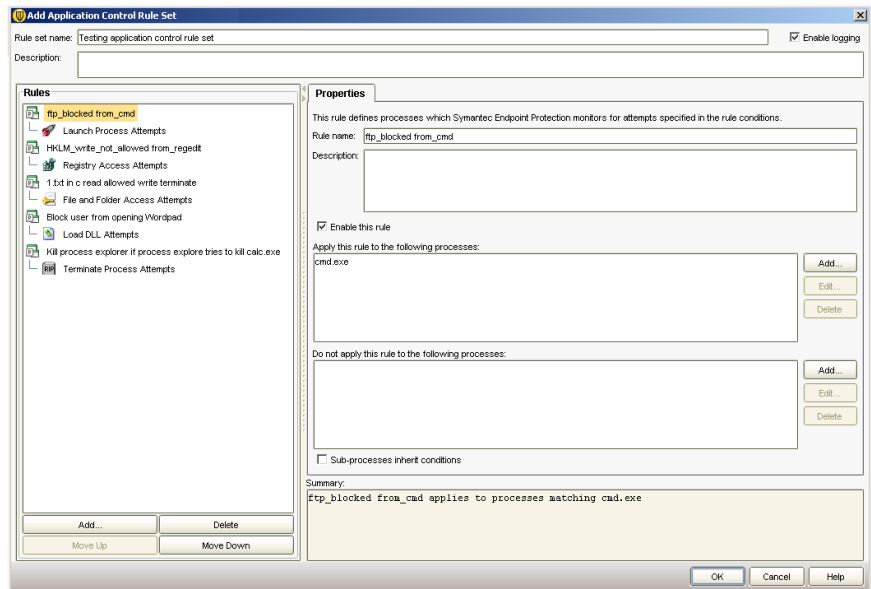
---

You can add and test a rule set that includes several rules that control an application on the client computer. You can add and test each rule one at a time, or add all the rules at once and test the rules later.

#### 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 56.
- 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.  
For example, change the name to **Testing the application control 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 Add the following rules:

- Add a rule that blocks FTP from being launched from the command prompt.  
See [“Adding and testing a rule that blocks a process from being launched”](#) on page 94.
- Add a rule that lets you to view but not edit a registry key.  
See [“Adding and testing a rule that blocks you from writing to the registry”](#) on page 95.
- Add a rule that lets you view but not edit a text file in Notepad.  
See [“Adding and testing a rule that blocks a DLL”](#) on page 96.
- Add a rule that blocks you from opening Microsoft WordPad.  
See [“Adding and testing a rule that allows or blocks access to a file”](#) on page 97.
- Add a rule that terminates the Process Explorer tool if the tool tries to terminate the Calculator.  
See [“Adding and testing a rule that terminates a process”](#) on page 98.



**10 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.

## Adding and testing a rule that blocks a process from being launched

The FTP client is a common way to transfer files from a server to a client computer. To prevent users from transferring files, you can add a rule that blocks a user from launching an FTP client from the command prompt.

### To add a rule that blocks a process from being launched

- 1 In the Add Application Control Rule Set dialog box, in the Rules list, select a rule, and on the Properties tab, in the Rule name text box, type **ftp\_blocked\_from\_cmd**.
- 2 To the right of Apply this rule to the following processes, click **Add**.
- 3 In the Add Process Definition dialog box, under Processes name to match, type **cmd.exe**, and then click **OK**.

- 4 In the Add Application Control Rule Set dialog box, under the Rules list, click **Add Condition > Launch Process Attempts**.
- 5 On the Properties tab, in the Description text box, type **no ftp from cmd**.
- 6 To the right of Apply this rule to the following processes, click **Add**.
- 7 In the Add Process Definition dialog box, under Processes name to match, type **ftp.exe**, and then click **OK**.
- 8 In the Add Application Control Rule Set dialog box, on the Actions tab, select **Block access**, and then check **Enable logging** and **Notify user**.
- 9 Under Notify user, type **ftp is blocked if launched from the cmd**.

**To test a rule that blocks a process from being launched**

- 1 On the client computer, open a command prompt.
- 2 In the command prompt window, type `ftp`, and then press **Enter**.

As the rule has specified, the FTP client does not open.

## **Adding and testing a rule that blocks you from writing to the registry**

You can protect a specific registry key by blocking the user from accessing or from modifying any registry keys or values in the registry. You can allow users to view the registry key, but not rename or modify the registry key.

To test the functionality:

- Add a test registry key.
- Add a rule to read but not write to the registry key.
- Try to add a new value to the registry key.

**To add a test registry key**

- 1 On the client computer, open the Registry Editor by opening a command line, then by typing `regedit`.
- 2 In the Registry Editor, expand `HKEY_LOCAL_MACHINE\Software`, and then create a new registry key called `test`.

**To add a rule that blocks you from writing to the registry**

- 1 In the Edit Application Control Rule Set, under the Rules list, click **Add > Add Rule**.
- 2 On the Properties tab, in the Rules name text box, type **HKLM\_write\_not\_allowed\_from\_regedit**.
- 3 To the right of Apply this rule to the following processes, click **Add**.

- 4 In the Add Process Definition dialog box, under Processes name to match, type **regedit.exe**, and then click **OK**.
- 5 In the Edit Application Control Rule Set dialog box, under the Rules list, click **Add Condition > Registry Access Attempts**.
- 6 On the Properties tab, in the Description text box, type **registry access**.
- 7 To the right of Apply this rule to the following processes, click **Add**.
- 8 In the Add Registry Key Definition dialog box, in the Registry key text box, type **HKEY\_LOCAL\_MACHINE\software\test**, and then click **OK**.
- 9 In the Edit Application Control Rule Set dialog box, on the Actions tab, in the Read Attempt group box, select **Allow access**, and then check **Enable logging** and **Notify user**.
- 10 Under Notify user, type **reading is allowed**.
- 11 In the Create, Delete, or Write Attempt group box, click **Block access**, and then check **Enable logging** and **Notify user**.
- 12 Under Notify user, type **writing is blocked**.

#### To test a rule that blocks you from writing to the registry

- 1 After you have applied the policy, on the client computer, in the Registry Editor, expand **HKEY\_LOCAL\_MACHINE\Software**.
- 2 Click the registry key that you created earlier, called **test**.
- 3 Right-click the test key, click **New**, and then click **String Value**.

You should not be able to add a new value to the test registry key.

## Adding and testing a rule that blocks a DLL

You may want to prevent the user from opening a specific application. One way to block a user from opening an application is to block a DLL that the application uses to run. To block the DLL, you can create a rule that blocks the DLL from loading. When the user tries to open the application, they cannot.

For example, the **Msvcr7.dll** file contains the program code that is used to run various Windows applications such as Microsoft WordPad. If you add a rule that blocks **Msvcr7.dll** on the client computer, you cannot open Microsoft WordPad.

#### To add a rule that blocks a DLL

- 1 In the Edit Application Control Rule Set, under the Rules list, click **Add > Add Rule**.
- 2 On the Properties tab, in the Rules name text box, type **Block user from opening Microsoft Wordpad**.

- 3 To the right of Apply this rule to the following processes, click **Add**.
- 4 In the Add Process Definition dialog box, under Processes name to match, type **C:\Program Files\Windows NT\Accessories\wordpad.exe**, and then click **OK**.
- 5 In the Edit Application Control Rule Set dialog box, under the Rules list, click **Add Condition > Load DLL Attempts**.
- 6 On the Properties tab, in the Description text box, type **dll launched**.
- 7 To the right of Apply this rule to the following processes, click **Add**.
- 8 In the Add DLL Definition dialog box, in the text box in the DLL name to match group box, type **MSVCRT.dll**, and then click **OK**.
- 9 In the Edit Application Control Rule Set, on the Actions tab, click **Block access**, and then check **Enable logging** and **Notify user**.
- 10 Under Notify user, type **Should not be able to load WordPad**.

**To test a rule that blocks a DLL**

- ◆ On the client computer, try to open Microsoft WordPad.

**Adding and testing a rule that allows or blocks access to a file**

You may want users to view but not modify a file. For example, a file may include the financial data that employees should view but not edit.

To test a rule that gives you read-only access to a file, add a rule that lets you open a text file in Notepad but does not let you edit it.

**To add a rule that allows or blocks access to a file**

- 1 In the Edit Application Control Rule Set, under the Rules list, click **Add > Add Rule**.
- 2 On the Properties tab, in the Rules name text box, type **1.txt in c read allowed write terminate**.
- 3 To the right of Apply this rule to the following processes, click **Add**.
- 4 In the Add Process Definition dialog box, under Processes name to match, type **notepad.exe**, and then click **OK**.
- 5 In the Edit Application Control Rule Set dialog box, under the Rules list, click **Add Condition > File and Folder Access Attempts**.
- 6 On the Properties tab, in the Description text box, type **file access launched**.
- 7 To the right of Apply this rule to the following processes, click **Add**.

- 8 In the Add File or Folder Definition dialog box, in the text box in the File or Folder Name To Match group box, type **c:\1.txt**, and then click **OK**
- 9 In the Edit Application Control Rule Set dialog box, on the Actions tab, in the Read Attempt group box, select **Allow access**, and then check **Enable logging** and **Notify user**.
- 10 Under Notify user, type **reading is allowed**.
- 11 In the Create, Delete, or Write Attempt group box, click **Terminate process**, and then check **Enable logging** and **Notify user**.
- 12 Under Notify user, type **writing to terminate Notepad**.

#### To test a rule that allows or blocks access to a file

- 1 On the client computer, open File Explorer, locate the c:\ drive, and then click **File > New > Text Document**.  
If you create the file by using Notepad, the file is a read-only file.
- 2 Rename the file as 1.txt.  
Make sure that the file is saved to the c:\ folder.
- 3 In Notepad, open the c:\1.txt file.  
You can open the file but you cannot edit it.

## Adding and testing a rule that terminates a process

Process Explorer is a tool that displays the DLL processes that have opened or loaded, and what resources the processes use. You can also use the Process Explorer to terminate a process. You can add a rule to terminate the Process Explorer if the user uses Process Explorer to try to terminate the Calculator application.

#### To add a rule that terminates a process

- 1 In the Edit Application Control Rule Set, under the Rules list, click **Add > Add Rule**.
- 2 On the Properties tab, in the Rules name text box, type **Terminates Process Explorer if Process Explorer tries to terminate calc.exe**.
- 3 To the right of Apply this rule to the following processes, click **Add**.
- 4 In the Add Process Definition dialog box, under Processes name to match, type **procexp.exe**, and then click **OK**.
- 5 In the Edit Application Control Rule Set dialog box, under the Rules list, click **Add Condition > Terminate Process Attempts**.
- 6 On the Properties tab, in the Description text box, type **dll launched**.

- 7 To the right of Apply this rule to the following processes, click **Add**.
- 8 In the Add Process Definition dialog box, in the text box in the Process name to match group box, type **calc.exe**, and then click **OK**.
- 9 In the Edit Application Control Rule Set, on the Actions tab, click **Terminate process**, and then check **Enable logging** and **Notify user**.
- 10 Under Notify user, type **If you try to terminate the calc from procexp, procexp terminates**.

**To test a rule that terminates a process**

- 1 On the client computer, download and run a free version of the Process Explorer from the following URL:  
<http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>
- 2 In Windows, open the Calculator.
- 3 Open the Process Explorer.
- 4 In the Process Explorer main window, right-click the calc.exe process, and then click **Kill Process**.

The Process Explorer is terminated.

## About device control

Use device control to manage peripheral devices' access to client computers. You can implement device control by constructing Hardware Device Control Lists. 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.

Device control gives an administrator a finer level of control over the devices that are allowed to access computers. Administrators can customize device control to block certain device types (such as all USB devices) from accessing computers. However, the administrator can also allow other device types (such as a USB hard drive) to be excluded from being blocked. The administrator can also choose to define device control by using either the Windows GUID or the device ID.

[Table 4-12](#) lists sample port and device configuration combinations and the effect each combination has on the device that tries to access the client computer.

**Table 4-12** Port and device configuration combinations

Configuration	Result
Port blocked + device excluded	Device works
Port excluded + device blocked	Device does not work <b>Note:</b> 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.

## 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.

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}
```

### About device IDs

A device ID is the most specific ID for a device. Devices can have either a specific device ID or a more generic ID. For example, you can specify all USB devices that use one device ID or you can choose one specific removable USB disk drive. You must use the device IDs for the devices that you want to add.

The following is a sample device ID:

```
{IDE\CDROMHL-DT-ST_RW/DVD_GCC-4242N_____0201____
\5&3CCF215&0&0.0.0}
```

## Obtaining a class ID or device ID

You can use the Symantec DevViewer tool to get either the class ID or the device ID. You can use Windows Device Manager to get the class ID.

### To obtain a class ID or device ID by using the DevViewer tool

- 1 On CD 3 of your product, locate the \TOOLS\NOSUPPORT\DEVVIEWER directory, 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.  
 For example, expand Keyboards and select the device within that category.
- 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 101.

## 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.

**To add hardware devices to the Hardware Devices list**

- 1 On the Symantec Endpoint Protection Manager 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.  
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 101.
- 6 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 hardware devices”](#) on page 100.

**To add device control to an Application and Device Control Policy**

- 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**.

### To test device control in an Application and Device Control Policy

- 1 In the console, add a hardware device to the Hardware Devices list for the client computer's keyboard.  
See [“Obtaining a class ID or device ID”](#) on page 101.
- 2 Assign the policy to the client computer's group.
- 3 On the client computer, try to type on the keyboard.



# Creating client installation packages

This chapter includes the following topics:

- [Creating client installation packages](#)
- [About client installation packages](#)
- [Configuring installation package features](#)
- [Configuring client installation package settings](#)
- [Exporting client installation packages](#)
- [Deploying client software with the Push Deployment Wizard](#)

## Creating client installation packages

You can use the following process to create an installation package and deploy it to the client computers. You should first set up groups and configure the policies and other security settings before you create a client installation package.

**Table 5-1** Process for setting up a client installation package

To perform this step	Action	See this section
Step 1	Read about client installation packages.	See <a href="#">“About client installation packages”</a> on page 106.
Step 2	Configure the client installation packages features and settings.	

**Table 5-1** Process for setting up a client installation package (*continued*)

To perform this step	Action	See this section
Step 3	Export the client installation package.	See <a href="#">“Exporting client installation packages”</a> on page 107.

## About client installation packages

To manage computers with the Symantec Endpoint Protection Manager Console, 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 CD.

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.

## Configuring 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.

#### To configure 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.

#### 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**.

## 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 MyGroup beneath Global, a directory named Global\_MyGroup 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.

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

#### 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, click the package to export.
- 4 Under Tasks, click **Export Client Install Package**.
- 5 In the Export Package dialog box, click **Browse**.
- 6 In the Select Export Folder dialog 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.

- 7 In the Export Package dialog box, set the other options according to your installation goals.
- 8 For details about setting other options in this dialog box, click **Help**.
- 9 Click **OK**.

## Deploying client software with the Push Deployment Wizard

The Push Deployment Wizard either appears automatically when you use the deployment wizard, or you can start it manually. Either way, you should have an idea of what client software package you want to deploy and in what folder the package exists. You have to locate it during deployment.

### To deploy client software with the Push Deployment Wizard

- 1 Start the Migration and Deployment Wizard from the Windows Start menu.
- 2 In the Welcome panel, click **Next**.
- 3 Click **Deploy the client** (Symantec Endpoint Protection only), and then click **Next**.
- 4 Click **Select an existing client install package to deploy**, and then click **Finish**.
- 5 In the Push Deployment Wizard panel, click **Browse**, navigate to and select the folder containing the install package you want to deploy, and then click **OK**.
- 6 Approve or modify the maximum number of concurrent deployments, and then click **Next**.
- 7 In the Select Computers panel, in the left pane under Available Computers, expand the trees and select the computers on which to install the client software, and then click **Add**.

As an alternative, you can import a workgroup or domain of computers, and also a text file list of computers.

- 8 In the Remote Client Authentication dialog box, type a user name and password that can authenticate to the Windows Domain or Workgroup that contains the computers, and then click **OK**.
- 9 When you have selected all of the computers and they appear in the right pane, click **Finish**.



# Configuring Host Integrity for endpoint compliance

This chapter includes the following topics:

- [Setting up and testing a Host Integrity Policy](#)
- [Adding Host Integrity requirements](#)
- [Adding a predefined firewall requirement](#)
- [Adding a custom requirement that checks whether the client computer runs an antivirus software package](#)
- [Testing to see if the Host Integrity Policy works](#)
- [Configuring peer-to-peer authentication](#)

## Setting up and testing a Host Integrity Policy

Symantec Network Access Control evaluates whether a laptop or desktop is a properly protected and compliant device before allowing it to connect to the corporate network. This protection helps prevent viruses and other attacks from entering the network through non-compliant clients. You can implement endpoint compliance on client computers by creating a Host Integrity Policy.

---

**Note:** You must have Symantec Network Access Control installed to create Host Integrity Policies.

---

To ensure endpoint compliance, the client computer uses the Host Integrity Policy to perform the following process:

**Table 6-1** Process that the client performs to ensure that the client computer is compliant with the Host Integrity Policy

To perform this step	Action	Description
Step 1	The client runs a Host Integrity check. The client compares the computer's configuration with the Host Integrity Policy that was downloaded from the management server.	The Host Integrity Policy checks whether the computer runs the most recent security software, patches, hotfixes, and other security requirements. For example, the policy may check how recently its antivirus definitions have been updated, and which were the latest patches applied to the operating system.
Step 2	Based on the result of the Host Integrity check, the client either allows or blocks the client computer from the network.	<ul style="list-style-type: none"> <li>■ If the computer meets all the policy's requirements, the Host Integrity check passes. The client computer has full network access to computers that pass the Host Integrity check.</li> <li>■ If the computer does not meet the policy's requirements, the Host Integrity check fails. When a Host Integrity check fails, the client blocks or quarantines the non-compliant computer until the user remediates the computer. You can set up a Quarantine Policy for quarantined client computers. Quarantined computers have limited or no access to the network.</li> </ul>
Step 3	The client remediates the non-compliant computer.	If the client finds that a Host Integrity Policy requirement is not met, it installs or requests the user to install the required software. After the client computer is remediated, it tries to access the network again. If the computer is fully compliant, the network grants the computer network access.

**Table 6-1** Process that the client performs to ensure that the client computer is compliant with the Host Integrity Policy (*continued*)

To perform this step	Action	Description
Step 4	The client proactively monitors compliance.	The client actively monitors the compliance state for all client computers. If at any time the computer's compliance status changes, so do the network access privileges of the computer.

To create and test a Host Integrity Policy, you can perform the following steps:

**Table 6-2** Process to set up and test a Host Integrity Policy

To perform this step	Description	See this section
Step 1	Create a predefined requirement or a custom requirement. The client compares each requirement with the software installed on the client computer.	See <a href="#">“Adding a predefined firewall requirement”</a> on page 115. See <a href="#">“Adding a custom requirement that checks whether the client computer runs an antivirus software package”</a> on page 116.
Step 2	Assign the policy to a group.	See <a href="#">“Assigning a shared policy”</a> on page 57.
Step 3	Test to see if the Host Integrity Policy works.	See <a href="#">“Testing to see if the Host Integrity Policy works”</a> on page 117.

## Adding Host Integrity requirements

A Host Integrity Policy sets the requirements for firewalls, antivirus, antispyware, patches, service packs, or other required applications on client computers.

Each Host Integrity Policy includes requirements and general settings. The requirements specify the following items:

- What conditions should be checked for
- What actions (such as downloads and installs) the client takes in response to the condition

When you specify Host Integrity requirements, you can choose from the following types: predefined, custom, or template requirements. Template requirements are

available through the Host Integrity Policy LiveUpdate service. You can copy and paste and export and import requirements between policies.

General settings enable you to configure when and how often the client runs a Host Integrity check, remediation options, and notifications.

You can create a new shared or non-shared Host Integrity Policy. After you create a new policy, you can add a predefined requirement, a custom requirement, or both.

#### To add a Host Integrity requirement

- 1 In the console, open a Host Integrity Policy.
- 2 On the Host Integrity Policy page, click **Requirements**.
- 3 On the Requirements page, select when the Host Integrity checks should run on the client from one of the following options:

Always do Host Integrity checking	This choice is the default. A Host Integrity check is always performed in this location at the frequency interval you specify.
Only do Host Integrity checking through the Gateway or DHCP Enforcer	A Host Integrity check is performed in this location only when the client is authenticated through a Gateway Enforcer or a DHCP Enforcer.
Only do Host Integrity checking when connected to the management server	A Host Integrity check is performed in this location only when the client is connected to a management server.
Never do Host Integrity checking	A Host Integrity check is never performed in this location.

- 4 Click **Add**.
- 5 In the Add Requirement dialog box, select one of the following requirement types:
  - Antivirus requirement
  - Antispyware requirement
  - Firewall requirement
  - Patch requirement
  - Service pack requirement
  - Custom requirement

- 6 Click **OK**.
- 7 Configure the settings for the requirement.
- 8 On the Advanced Settings page, configure settings for Host Integrity checks, remediation, and notifications.  
For more information, click **Help**.
- 9 When you are done with the configuration of the policy, click **OK**.
- 10 Assign the policy to groups or locations.  
See [“Assigning a shared policy”](#) on page 57.

## Adding a predefined firewall requirement

You can create a Host Integrity requirement that checks whether the Symantec Endpoint Protection client is installed and that the Network Threat Protection component runs. If you have already installed the client, the check for this Host Integrity requirement passes. If you have not yet installed the client, or if you disable Network Threat Protection on the client, this requirement fails. However, you can configure the requirement to pass anyway.

### To add a predefined patch requirement

- 1 In the console, open a Host Integrity Policy.
- 2 On the Host Integrity Policy page, click **Requirements**.
- 3 On the Requirements page, click **Always do Host Integrity checking**, and then click **Add**.
- 4 In the Add Requirement dialog box, click **Firewall requirement**, and then click **OK**.
- 5 In the Add Requirement dialog box, in the Name text box, type **Check that the SEP firewall is running**.
- 6 In the Firewall application that must be installed and running drop-down list, click **Symantec Endpoint Protection**.
- 7 To enable the requirement to pass even if the check fails, check **Allow the Host Integrity check to pass even if this requirement fails**.
- 8 Click **OK**.
- 9 On the Overview page, click **OK**.
- 10 If the policy is not already assigned to a group or location, assign the policy.  
See [“Assigning a shared policy”](#) on page 57.

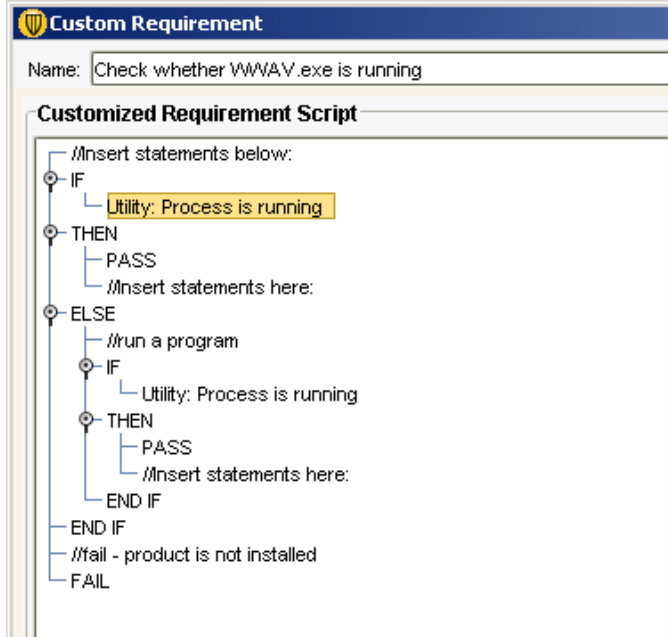
## Adding a custom requirement that checks whether the client computer runs an antivirus software package

You can configure a Host Integrity Policy to check whether a known software package is running on the client computer.

### To check whether the product is running

- 1 Add a custom requirement.
- 2 In the Custom Requirement dialog box, type a name for the requirement.
- 3 Under Customized Requirement Script, click **Add**, and then click **IF..THEN...**
- 4 With the IF node selected, in the right-hand pane, under Select a condition, click **Utility: Process is running**.
- 5 In the Process file name text box, type **C:\Program Files\WidgetWorks\WWAV.exe**.
- 6 Under Customized Requirement Script, select THEN, click **Add**, and then click **Return**.
- 7 Select THEN, click **Add**, and then click **Else**.
- 8 Under the Else node, select //Insert statements here, and in the right-hand pane, type **Run the program**.
- 9 Under Customized Requirement Script, click **Add**, and then click **IF..THEN...**
- 10 In the Select a condition drop-down list, click **Utility: Process is running**.
- 11 In the Process file name text box, type **WWAV**.
- 12 Under Customized Requirement Script, select THEN, click **Add**, and then click **Return**.
- 13 Select the END IF under the first END IF, click **Add**, and then click **Comment**.
- 14 In the Comment text box, type **fail – product is not installed**.

- 15 Under Customized Requirement Script, select PASS, and in the right-hand pane, click **Fail**.



- 16 Click **OK**.
- 17 To enable the requirement to pass even if the check fails, check **Allow the Host Integrity check to pass even if this requirement fails**.
- 18 When you are done with the configuration of the policy, click **OK**.

## Testing to see if the Host Integrity Policy works

To test if the Host Integrity Policy works, you can use the following process:

**Table 6-3** Process to test the Host Integrity Policy

To perform this step	Description	See this section
Step 1	Check to see that the policy is updated on the clients. You can also update the policy on the client.	See <a href="#">“Verifying that policies have been updated”</a> on page 58. See <a href="#">“Updating the policy file manually”</a> on page 58.

**Table 6-3** Process to test the Host Integrity Policy (*continued*)

To perform this step	Description	See this section
Step 2	Run the Host Integrity check.	See <a href="#">“Running a Host Integrity check”</a> on page 118.
Step 3	View the Security log to see if the Host Integrity check passed or failed.	See <a href="#">“Viewing the Network Access Control logs”</a> on page 118.

## Running a Host Integrity check

Your administrator configures the frequency that the client uses to run a Host Integrity check. You may need to run a Host Integrity check immediately rather than wait for the next check. For example, a failed Host Integrity check may find that you need to update the antivirus application on your computer. The client may allow you to choose whether to download the required software immediately or postpone the download. If you download the software immediately, you must run the Host Integrity check again to verify that you have the correct software. You can either wait until the next scheduled Host Integrity check runs or you can run the check immediately.

### To run a Host Integrity check

- 1 In the client, in the sidebar, click **Status**.
- 2 Next to Network Access Control, click **Options > Check Now**.
- 3 If a message appears that confirms that the Host Integrity check ran, click **OK**.

If you had been blocked from network access, you should regain network access when your computer has been updated to comply with the security policy.

## Viewing the Network Access Control logs

The Symantec Network Access Control client uses the following logs to monitor different aspects of its operation and the Host Integrity check:

Security	Records the results and status of Host Integrity checks.
System	Records all operational changes for the client, such as the connection to the management server and updates to the client security policy.

If you use a managed client, both of the logs may be regularly uploaded to the server. Your administrator can use the content in the logs to analyze the overall security status of the network.

You can export the log data from these logs.

#### To view Symantec Network Access Control logs

- 1 In the client, in the sidebar, click **Status**.
- 2 To view the System Log, next to Network Access Control, click **Options > View Logs**.
- 3 To view the Security Log, in the Client Management Logs - System log dialog box, click **View > Security Log**.
- 4 In the Security Log, select the top log entry.  
In the lower-left corner, the Host Integrity check results appear. If the client was already installed, the predefined firewall requirement passes. If the client was not installed, the predefined firewall requirement fails but is reported as having passed.
- 5 Click **File > Close**.

## 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.
- 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 57.

# Using logs and reports to monitor security

This chapter includes the following topics:

- [About logs and reports](#)
- [About the Symantec Endpoint Protection Home page](#)
- [About logs](#)
- [Viewing logs](#)
- [Running commands and actions from logs](#)
- [Using notifications](#)
- [Creating quick reports](#)

## About logs and reports

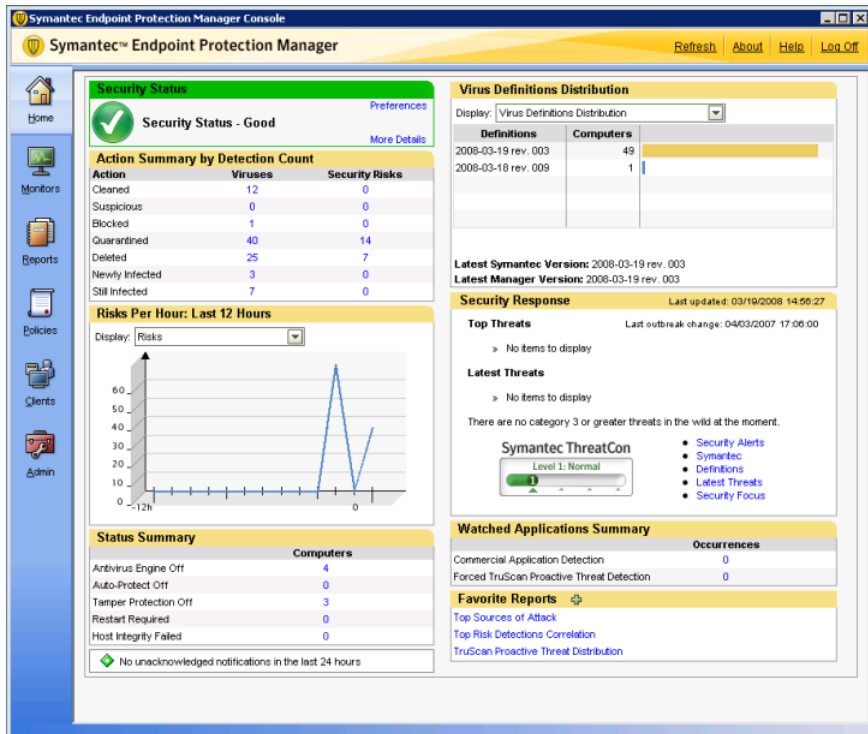
The reporting functions give you the up-to-date information that you need to monitor and make informed decisions about the security of your network. The Symantec Endpoint Protection Manager Console Home page displays the automatically generated charts that contain information about the important events that have happened recently in your network. You can use the filters on the Monitors page to view more detailed, real-time information about your network from the logs. 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.

# 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.

Figure 7-1 shows a sample Home page that the administrators that have permission to view reports see.

Figure 7-1 Sample Symantec Endpoint Protection Home page on the Symantec Endpoint Protection Manager Console



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 7-1](#) describes each item on the Symantec Endpoint Protection Home page in detail.

**Table 7-1** 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.  You can click the security status icon on the Home page for details.

**Table 7-1** Home page items and reports (*continued*)

Report or Status Information	Description
<p><i>Action Summary by Detection Count</i>    <i>Action Summary by Number of Computers</i></p>	<p>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.</p> <p>The Action Summary by Detection Count summarizes the following information:</p> <ul style="list-style-type: none"> <li>■ A count of the actions that have been taken on viruses and security risks.</li> <li>■ The incidence of new virus and security risk detections.</li> <li>■ The number of computers that remain infected by viruses and security risks.</li> </ul> <p>The Action Summary by Number of Computers summarizes the following information:</p> <ul style="list-style-type: none"> <li>■ The number of distinct computers on which the various actions have been performed on viruses and security risks.</li> <li>■ The total number of new virus and security risk detections.</li> <li>■ The total number of computers that still remain infected by viruses and security risks.</li> </ul> <p>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.</p> <p>For any of the actions, click the number of viruses or security risks to see a detailed report.</p> <p>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.</p>

**Table 7-1** Home page items and reports (*continued*)

Report or Status Information	Description
<p><i>Action Summary by Detection Count</i>    <i>Action Summary by Number of Computers</i>  (Continued)</p>	<p>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.</p> <p>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.</p> <p><b>Note:</b> 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.</p> <p>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.</p> <p>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.</p> <p><b>Note:</b> 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.</p> <p>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.</p> <p>See "<a href="#">Viewing logs</a>" on page 133.</p>

**Table 7-1** Home page items and reports (*continued*)

Report or Status Information	Description
<p><i>Attacks   Risks   Infections Per Hour: Last 12 Hours   Per Hour: Last 24 Hours</i></p>	<p>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:</p> <ul style="list-style-type: none"> <li>■ Attacks represent the incidents that Network Threat Protection thwarted.</li> <li>■ Risks represent all the antivirus, antispyware, and TruScan proactive threat scan detections that were made.</li> <li>■ Infections represent the viruses and security risks that were detected, but cannot be properly remediated.</li> </ul> <p>You can change the display by clicking a new view in the list box.</p> <p><b>Note:</b> You can click the Preferences link to change the default time interval that is used.</p>
<p>Notification status summary</p>	<p>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.</p> <p>See <a href="#">“Creating administrator notifications”</a> on page 141.</p>
<p>Status Summary</p>	<p>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:</p> <ul style="list-style-type: none"> <li>■ The Antivirus Engine is turned off.</li> <li>■ Auto-Protect is turned off.</li> <li>■ Tamper Protection is turned off.</li> <li>■ The computers require a restart to complete some form of risk remediation or to complete the installation of a LiveUpdate software download.</li> <li>■ The computers have failed a host integrity check. This number is always zero if you do not have Symantec Network Access Control installed.</li> </ul> <p>You can click each number in the Status Summary for details.</p> <p>The number of unacknowledged notifications in the last 24 hours also appears.</p>
<p><i>Virus Definitions Distribution   Intrusion Prevention Signatures</i></p>	<p>The Virus Definitions Distribution and Intrusion Prevention Signatures section of the Home page shows how the current virus definitions and IPS signatures are distributed.</p> <p>You can toggle between them by clicking a new view in the list box.</p>

Table 7-1 Home page items and reports (*continued*)

Report or Status Information	Description
Security Response	<p>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.</p> <p>You can click any of the links to get additional information.</p> <p><b>Note:</b> 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.</p>
Watched Applications Summary	<p>The Watched Applications Summary shows the occurrences of applications in your network that are on the following lists:</p> <ul style="list-style-type: none"> <li>■ The Symantec Commercial Applications list</li> <li>■ The Forced TruScan Proactive Threat Detection list, which is your custom list of watched applications</li> </ul> <p>You can click a number to display a more detailed report.</p>
Favorite Reports	<p>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.</p> <p>To select the reports that you want to access from the Home page, you can click the plus icon beside Favorite Reports.</p>

You can use the Preferences link to change the time period for the reports and the summaries that display on those pages. The default is the past 24 hours; the other option is the past week. You can also change the default reports that are displayed in the Favorite Reports section of the Home page.

## About logs

Using the logs, you can view detailed events from your security products. 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 may want to view this information to troubleshoot security or connectivity problems in your network. This information may also be useful for the investigation of threats or to verify the history of events.

---

**Note:** 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 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 for importing into a spreadsheet application. Other log data can be exported to a dump file or a Syslog server.

## About log types, contents, and commands

You can view the following types of logs from the Monitors page:

- Application and Device Control
- Audit
- Compliance
- Computer Status
- Network Threat Protection
- TruScan Proactive Threat Scan
- Risk
- Scan
- System

---

**Note:** All these logs are accessed from the Monitors page by using the Logs tab. You can view information about the created notifications on the Notifications tab and information about the status of commands on the Command Status 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.

See [“Viewing and filtering administrator notification information”](#) on page 139.

---

**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.

---

[Table 7-2](#) describes the different types of content that you can view and the actions that you can take from each log.

**Table 7-2** Log and lists

Log type	Contents and actions
Application and Device Control	<p>The Application Control log and the Device Control log contain information about events where some type of behavior was blocked.</p> <p>The following Application and Device Control logs are available:</p> <ul style="list-style-type: none"> <li>■ Application Control, which includes information about Tamper Protection</li> <li>■ Device Control</li> </ul> <p>The information that is available in the Application Control log includes such items as the following:</p> <ul style="list-style-type: none"> <li>■ The time the event occurred</li> <li>■ The action taken</li> <li>■ The domain and computer that were involved</li> <li>■ The severity</li> <li>■ The rule that was involved</li> <li>■ The caller process</li> <li>■ The target</li> </ul> <p>The information that is available in the Device Control log includes such items as the following:</p> <ul style="list-style-type: none"> <li>■ The time the event occurred</li> <li>■ The event type</li> <li>■ The domain and group that were involved</li> <li>■ The computer that was involved</li> <li>■ The user that was involved</li> <li>■ The operating system name</li> <li>■ A description</li> <li>■ The location</li> <li>■ The name of the application that was involved</li> </ul> <p>You can add a file to a Centralized Exceptions Policy from the Application Control log.</p>

**Table 7-2** Log and lists (*continued*)

Log type	Contents and actions
Audit	<p>The Audit log contains information about policy modification activity. Available information includes the event time and type; the policy modified; the domain, site, and administrator involved; and a description.</p> <p>No actions are associated with this log.</p>
Compliance	<p>The compliance logs contain information about the Enforcer server, Enforcer clients, and Enforcer traffic, and about host compliance.</p> <p>The following compliance logs are available if you have Symantec Network Access Control installed:</p> <ul style="list-style-type: none"> <li>■ <b>Enforcer Server</b>  This log tracks communication between Enforcers and their management server. Information that is logged includes the Enforcer name, when it connects to the management server, the event type, site, and server name.</li> <li>■ <b>Enforcer Client</b>  Provides the information on all Enforcer client connections, including peer-to-peer authentication information. Available data includes each Enforcer's name, type, site, remote host, and remote MAC address, and whether or not the client was passed, rejected, or authenticated.</li> <li>■ <b>Enforcer Traffic (Gateway Enforcer only)</b>  Provides some information about the traffic that moves through an Enforcer appliance. This information includes the direction and time of the traffic, the protocol that was used, the Enforcer name and site. The information also includes the local port that was used, the direction, and a count. You can filter on the connection attempts that were allowed or blocked.</li> <li>■ <b>Host Compliance</b>  This log tracks the details of host integrity checks of clients. Available information includes the time, location, operating system, reason for failures, and a description.</li> </ul> <p>No actions are associated with these logs.</p>

Table 7-2 Log and lists (*continued*)

Log type	Contents and actions
Computer Status	<p>The Computer Status log contains information about the real-time operational status of the client computers in the network. Information available includes the computer name and IP address, last checkin time, definitions date, infected status, Auto-Protect status, server, group, domain, and user name.</p> <p>You can perform the following actions from the Computer Status log:</p> <ul style="list-style-type: none"> <li>■ <b>Scan</b> 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.</li> <li>■ <b>Update Content</b> This command triggers an update of policies, definitions, and software from the Symantec Endpoint Protection Manager Console to the clients in the selected group.</li> <li>■ <b>Update Content and Scan</b> This command triggers an update of the policies, definitions, and software on the clients in the selected group. This command then launches a 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.</li> <li>■ <b>Cancel All Scans</b> This command cancels all running scans and any queued scans on the selected recipients.</li> <li>■ <b>Restart Client Computers</b> 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.</li> <li>■ <b>Enable Auto-Protect</b> This command turns Auto-Protect on for all the client computers that you selected.</li> <li>■ <b>Enable Network Threat Protection</b> This command turns on Network Threat Protection for all the client computers that you selected.</li> <li>■ <b>Disable Network Threat Protection</b> This command turns Network Threat Protection off for all the client computers that you selected.</li> </ul> <p>You can also clear the infected status of computers from this log.</p>

**Table 7-2** Log and lists (*continued*)

Log type	Contents and actions
Network Threat Protection	<p>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 contains some of the operational changes that are made to computers, such as detecting network applications, and configuring software. Information available includes items such as the time, the event type; and the action taken. Additional information available includes the severity; the direction, the host name, the action taken, the IP address, and the protocol involved.</p> <p>The following Network Threat Protection logs are available:</p> <ul style="list-style-type: none"> <li>■ Attacks</li> <li>■ Traffic</li> <li>■ Packet</li> </ul> <p>No actions are associated with these logs.</p>
TruScan Proactive Threat Scan	<p>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 name, computer and user involved, the application name and type, and the file name.</p> <p>You can add a detected process to a preexisting Centralized Exceptions Policy from this log.</p>
Risk	<p>The Risk log contains information about risk events. Some of the information available includes the event name and time, user name, computer, risk name, count, source, and path name.</p> <p>You can take the following actions from this log:</p> <ul style="list-style-type: none"> <li>■ Add Risk to Centralized Exceptions Policy</li> <li>■ Add File to Centralized Exceptions Policy</li> <li>■ Add Folder to Centralized Exceptions Policy</li> <li>■ Add Extension to Centralized Exceptions Policy</li> <li>■ Delete from Quarantine</li> </ul>
Scan	<p>The Scan log contains information about antivirus and antispysware scan activity. Information available includes items such as the computer name, IP address, status, scan time, duration, and scan results.</p> <p>No actions are associated with these logs.</p>

Table 7-2 Log and lists (continued)

Log type	Contents and actions
System	<p>The system logs contain information about events such as when services start and stop. Information available includes items such as event time and event type; the site, domain, and server involved; and severity.</p> <p>The following system logs are available:</p> <ul style="list-style-type: none"><li>■ Administrative</li><li>■ Client-Server Activity</li><li>■ Server Activity</li><li>■ Client Activity</li><li>■ Enforcer Activity</li></ul> <p>No actions are associated with these logs.</p>
Command Status list	<p>The Command Status list contains information about the status of commands that you have run from the console. It includes information such as the date the command was run, who issued it, and a description of the command. It also includes the completion status of the command and the clients that the command affected.</p>
Notifications list	<p>The Notifications list contains information about notification events. Such events include information such as the date and time of the notification. It also includes whether or not the notification was acknowledged, who created it, its subject, and the message.</p> <p>No actions are associated with these logs.</p> <p><b>Note:</b> The Notifications log is accessed from the Notifications tab on the Monitors page, not from the Logs tab.</p> <p>See <a href="#">“Viewing and filtering administrator notification information”</a> on page 139.</p>

## 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 has 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.

---

**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.

If you get CGI or terminated process errors, you might want to change other timeout parameters.

For 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, Auto-Refresh has no effect. The data always stay the same.

---

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. 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.
- 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.

### 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.

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.

- 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**.

## Running commands and actions from logs

From the Computer Status log, you can run several commands on selected clients.

You can also right-click a group directly from the Client 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 Scan 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

To add any type of exception from a log, you must already have created a Centralized Exceptions Policy.

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**.

## 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 141.

## 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
- Acknowledgment status
- Type
- Creator
- 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 acknowledgment 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.

## Creating administrator notifications

You can create and configure notifications to be triggered when certain security-related events occur.

You can configure the software 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.

[Table 7-3](#) describes the different types of events that trigger different types of notifications.

**Table 7-3** 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 change	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 7-3** 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 computer	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.

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 **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 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*.

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*

- 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.

## About editing existing notifications

If you edit the settings of an existing notification, the previous entries that it generated 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.

## Creating quick reports

Generate a quick report by selecting from the Basic 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 that you can configure, 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.

---

[Table 7-4](#) describes all the Basic Settings available for all types of quick report.

**Table 7-4** Basic filter settings for quick reports

Setting	Description
Time range	<p>Specifies the time range of events you want to view in the report.</p> <p>Select from the following times:</p> <ul style="list-style-type: none"> <li>■ Past 24 hours</li> <li>■ Past week</li> <li>■ Past month</li> <li>■ Current month</li> <li>■ Past three months</li> <li>■ Past year</li> <li>■ Set specific dates</li> </ul> <p>If you choose <b>Set specific dates</b>, some reports require that you set a <b>Start date</b> and <b>End date</b>. Other reports require that you set the <b>Last checkin time</b>, which is the last time that the computer checked in with its server.</p> <p>The default is <b>Past 24 hours</b>.</p>
Start date	<p>Specifies the start date for the date range.</p> <p>Only available when you select <b>Set specific dates</b> for the time range.</p>
End date	<p>Specifies the end date for the date range.</p> <p>Only available when you select <b>Set specific dates</b> for the time range.</p> <p><b>Note:</b> You cannot set an end date that is the same as the start date or earlier than the start date.</p>

**Table 7-4** Basic filter settings for quick reports (*continued*)

Setting	Description
Last checkin after	<p>Specifies that you want to see all entries that involve a computer that has not checked in with its server since this time.</p> <p>Only available for Computer Status reports when you select Set specific dates for the time range.</p>
Status	<p>Available for the Network Compliance Status Compliance report. Select from the following:</p> <ul style="list-style-type: none"><li>■ Authenticated</li><li>■ Disconnected</li><li>■ Failed</li><li>■ Passed</li><li>■ Rejected</li></ul> <p>Available for the Compliance Status Compliance report. Select from the following actions:</p> <ul style="list-style-type: none"><li>■ Passed</li><li>■ Failed</li></ul>
Group By	<p>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.</p>

**Table 7-4** Basic filter settings for quick reports (*continued*)

Setting	Description
Target	<p>Available for the Top Targets Attacked Network Threat Protection report. Select from the following:</p> <ul style="list-style-type: none"> <li>■ Group</li> <li>■ Subnet</li> <li>■ Client</li> <li>■ Port</li> </ul> <p>Available for the Attacks Over Time Network Threat Protection report. Select from the following:</p> <ul style="list-style-type: none"> <li>■ All</li> <li>■ Group</li> <li>■ IP Address</li> <li>■ Operating System</li> <li>■ User Name</li> <li>■ Attack Type</li> </ul> <p>Available for the Blocked Applications Over Time and Traffic Notifications Over Time Network Threat Protection reports. Select from the following:</p> <ul style="list-style-type: none"> <li>■ All</li> <li>■ Group</li> <li>■ IP Address</li> <li>■ Operating System</li> <li>■ User Name</li> </ul> <p>Available for the Top Traffic Notifications Network Threat Protection report. Select from the following:</p> <ul style="list-style-type: none"> <li>■ All</li> <li>■ Traffic</li> <li>■ Packet</li> </ul>
X-axis Y-axis	<p>Available for the Top Risk Detections Correlation Risk report. Select from the following:</p> <ul style="list-style-type: none"> <li>■ Computer</li> <li>■ User Name</li> <li>■ Domain</li> <li>■ Group</li> <li>■ Server</li> <li>■ Risk Name</li> </ul>
Bin width	<p>Specifies the width of a bin for forming a histogram. Available for the Scan Statistics Histogram Scan report.</p>

**Table 7-4** Basic filter settings for quick reports (*continued*)

Setting	Description
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 for that type of report on the console. Clicking Tell me more displays the context-sensitive Help for that type of report.

#### 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. For example, select Risk.
- 3 Under What type of Scan Report would you like to see, in the Select a report list box, select the name of the report you want to view. For example, select Risk Detections Count.
- 4 In the Use 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 selected 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.
- 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 on the Quick Reports tab to see descriptions of the filter options in the context-sensitive Help.

When the 3-dot button is available, it takes you to a list of known options for that choice. For example, this option can take you to a list of known servers or a list of known domains.

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**.

