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

Symantec.

Symantec Endpoint Protection and Symantec Network Access Control Installation and Administration 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.

Product version: 12.1.2

Documentation version: 12.1.2, version 1

Legal Notice

Technical Support

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

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

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

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

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

Support agreement resources

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

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

Contents

Section 3   Managing protection and customizing policies

Chapter 15   Using policies to manage security

Chapter 16   Managing Virus and Spyware Protection

Chapter 25   Monitoring protection with reports and logs 603

Chapter 26   Managing notifications 633

Section 5 Configuring and managing Symantec Endpoint Protection Manager 693

Chapter 32 Managing the connection between the management server and the client computers 695

Chapter 33 Configuring the management server 715

Chapter 51 Introducing the Symantec Integrated Enforcers 983

Chapter 52 Installing the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers 985

Chapter 55 **Installing the Symantec Integrated Enforcer for Microsoft Network Access Protection** 1025

Chapter 56 **Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console** 1033

Chapter 57   Configuring the Symantec Network Access Control
                  Integrated Enforcer for Microsoft Network
                  Access Protection on the Symantec Endpoint
                  Protection Manager 1041

Chapter 58   Setting up temporary connections for Symantec
                  Network Access Control On-Demand clients 1047

Introducing Symantec Endpoint Protection

This chapter includes the following topics:

- About Symantec Endpoint Protection

- What's new in Symantec Endpoint Protection 12.1.2

- About the types of threat protection that Symantec Endpoint Protection provides

- Protecting your network with Symantec Endpoint Protection

- Getting up and running on Symantec Endpoint Protection for the first time

- Managing protection on client computers

- Maintaining the security of your environment

- Troubleshooting Symantec Endpoint Protection

About Symantec Endpoint Protection

Symantec Endpoint Protection is a client-server solution that protects laptops, desktops, Windows and Mac computers, and servers in your network against malware. Symantec Endpoint Protection combines virus protection with advanced threat protection to proactively secure your computers against known and unknown threats.

Symantec Endpoint Protection protects against malware such as viruses, worms, Trojan horses, spyware, and adware. It provides protection against even the most sophisticated attacks that evade traditional security measures, such as rootkits, zero-day attacks, and spyware that mutates. Providing low maintenance and high

power, Symantec Endpoint Protection communicates over your network to automatically safeguard for both physical systems and virtual systems against attacks.

This comprehensive solution protects confidential and valuable information by combining multiple layers of protection on a single integrated client. Symantec Endpoint Protection reduces management overhead, time, and cost by offering a single management console for clients.

See "About the types of threat protection that Symantec Endpoint Protection provides" on page 46.

What's new in Symantec Endpoint Protection 12.1.2

Table 1-1 describes the new features in the latest version of Symantec Endpoint Protection.

Table 1-1   New features in Symantec Endpoint Protection 12.1.2

Feature	Description
System requirements	Symantec Endpoint Protection now supports additional new platforms and configurations.
	You can now install Symantec Endpoint Protection Manager on the following operating systems:
	■ Windows 8
	■ Windows Server 2012
	You can now install the Symantec Endpoint Protection client on the following operating systems:
	■ Windows 8 and Windows Server 2012
	■ Mac OS X 10.8, Mountain Lion
	■ Mac OS X case-sensitive formatted volumes
	You can now use Symantec Endpoint Protection Manager from the following browsers:
	■ Microsoft Internet Explorer 10
	■ Google Chrome
	For the complete list of system requirements:
	See "System requirements for Symantec Endpoint Protection" on page 75.
	See the knowledge base article: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

| | Table 1-1 | New features in Symantec Endpoint Protection 12.1.2 *(continued)* |

Feature	Description
Installation	The Client Deployment Wizard includes the following changes: ■ The Client Deployment Wizard includes the **Communication Update Package Deployment** option to push the communications file (Sylink.xml) to the client in a client installation package. You use the Sylink.xml file to convert an unmanaged client to a managed client, or to manage a previously orphaned client. In previous releases, you needed to export the Sylink.xml file from the management server, and import Sylink.xml to each client. See "Restoring client-server communications by using a client installation package" on page 701. See "Why do I need to replace the client-server communications file on the client computer?" on page 698. ■ The Client Deployment Wizard searches the network faster to find the computers that do not have the client software installed. ■ The Client Deployment Wizard includes the **Automatically uninstall existing security software** option so that a security software removal feature can uninstall third-party security products from the client computer. The feature removes security software before the client installation package installs the client software. With version 12.1.2, the feature removes more than 40 additional third-party products. For a list of products that the third-party security software removal feature uninstalls, see the knowledge base article: About the third-party security software removal feature in Symantec Endpoint Protection 12.1 See "Deploying clients using a Web link and email" on page 132. See "Deploying clients by using Remote Push" on page 135. See "Deploying clients by using Save Package" on page 137. You can download and run a new diagnostic tool on the management server and client to help you diagnose common issues before and after installation. The Symantec Help tool enables you to resolve product issues yourself instead of calling Support. See "Troubleshooting computer issues with the Symantec Help support tool" on page 755. See the knowledge base article at the following URL: Symantec Help (SymHelp)

| Table 1-1 | New features in Symantec Endpoint Protection 12.1.2 *(continued)* |

Feature	Description

Virtualization	Symantec Endpoint Protection includes the following virtualization improvements:
	
	■ A VMware vShield-enabled Shared Insight Cache. Delivered in a Security Virtual Appliance, you can deploy the vShield-enabled Shared Insight Cache into a VMware infrastructure on each host. The vShield-enabled Shared Insight Cache makes file scanning more efficient. You can monitor the Security Virtual Appliance and client status in Symantec Endpoint Protection Manager.
	See "What do I need to do to use a vShield-enabled Shared Insight Cache?" on page 668.
	■ For managing Guest Virtual Machines (GVMs) in non-persistent virtual desktop infrastructures:
	  ■ Symantec Endpoint Protection Manager includes a new option to configure the aging period for offline non-persistent GVMs. Symantec Endpoint Protection Manager removes the non-persistent GVM clients that have been offline longer than the specified time period.
	  ■ Symantec Endpoint Protection clients now have a configuration setting to indicate that they are non-persistent GVMs. You can filter out the offline non-persistent GVMs in the **Clients** tab view in Symantec Endpoint Protection Manager.
	See "Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures" on page 689.

Remote management	Symantec Endpoint Protection provides public support to remotely manage and monitor the client and the management server. New Web services let you write your own tools to perform the following tasks remotely: ■ Run commands on the client to remediate threat situations. ■ Export policies from the server. ■ Apply policies to clients across servers. ■ Monitor license status and content status on the management server. Documentation and other tools for remote monitoring and management support appear in the Web services SDK, located in the following folder on the installation disc: `/Tools/Integration/SEPM_WebService_SDK`
Windows 8 features	■ Support for the Microsoft Windows 8 style user interface, including toast notifications for critical events. See "Configuring user interface settings" on page 242. ■ Support for Windows 8 and Windows Server 2012. ■ Windows 8 Early Launch Anti-Malware (ELAM) support provides a Microsoft-supported way for anti-malware software to start before all other third-party components. In addition, vendors can now control the launching of third-party drivers, depending on trust levels. If a driver is not trusted, it can be removed from the boot sequence. ELAM support makes more efficient rootkit detection possible. See "Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options" on page 373.

| Table 1-1 | New features in Symantec Endpoint Protection 12.1.2 *(continued)* |

Feature	Description
Protection features	Virus and Spyware Protection:
	■ Full support for the Microsoft Windows 8 style user interface.
	Proactive Threat Protection:
	■ Device Control now sends a notification and creates a log event each time it blocks a previously disabled device. Previously, Device Control sent a notification and log event only the first time the device was disabled. See "Managing device control" on page 521.
	■ System lockdown can now run in blacklist mode. You must configure system lockdown to display a blacklist mode as well as the default whitelist mode. The blacklist mode blocks only the applications on the specified list. Symantec Endpoint Protection Manager can automatically update the existing file fingerprint lists and application name lists that system lockdown uses for whitelisting or blacklisting. See "Automatically updating whitelists or blacklists for system lockdown" on page 509.
	Exceptions:
	■ Added support for HTTPS in trusted Web domain exceptions.
	■ Common variables in exceptions now apply to 64-bit applications as well as 32-bit applications. See "Excluding a file or a folder from scans" on page 534.
	Policies:
	■ You can export all the policies, locations, and server settings for a domain. If you then import these policies and settings into a new domain, you do not need to recreate them. See "Exporting and importing server settings" on page 719. See "Adding a domain" on page 267. See "Exporting and importing individual policies" on page 303.
LiveUpdate	The LiveUpdate Settings policy includes an additional type of Group Update Provider (GUP) that allows clients to connect to Group Update Providers in a different subnet. This new type of GUP lets you explicitly define which networks each client may connect to. You can configure a single LiveUpdate policy to meet all your requirements.
	See "Using Group Update Providers to distribute content to clients " on page 580.
	A link on the client **Status** page now lets end users quickly and easily confirm that the client has the most current content. The link displays the content version dialog box, where a new column lists the last time that the client checked each content type for updates. Users can be more confident that their client updates correctly and has the latest protection.

About the types of threat protection that Symantec Endpoint Protection provides

You need combinations of all the protection technologies to fully protect and customize the security in your environment. Symantec Endpoint Protection combines traditional scanning, behavioral analysis, intrusion prevention, and community intelligence into a superior security system.

Table 1-2 describes the types of protection that the product provides and their benefits.

Table 1-2   Layers of protection

Protection type	Description	Benefit
Virus and Spyware Protection	Virus and Spyware Protection protects computers from viruses and security risks, and in many cases can repair their side effects. The protection includes real-time scanning of files and email as well as scheduled scans and on-demand scans. Virus and spyware scans detect viruses and the security risks that can put a computer, as well as a network, at risk. Security risks include spyware, adware, and other malicious files. See "Managing scans on client computers" on page 323.	Virus and Spyware Protection detects new threats earlier and more accurately using not just signature-based and behavioral-based solutions, but other technologies as well. ■ Symantec Insight provides faster and more accurate malware detection to find the new and the unknown threats that other approaches miss. Insight identifies new and zero-day threats by using the collective wisdom of millions of systems in hundreds of countries. ■ Bloodhound uses heuristics to detect known and unknown threats. ■ Auto-Protect scans files from a signature list as they are read from or written to the client computer.

Table 1-2 Layers of protection *(continued)*

Protection type	Description	Benefit
Network Threat Protection	Network Threat Protection provides a firewall and an intrusion prevention system to prevent intrusion attacks and malicious content from reaching the computer that runs the client software. The firewall allows or blocks network traffic based on the various criteria that the administrator sets. If the administrator permits it, end users can also configure firewall policies. The Intrusion Prevention System (IPS) analyzes all the incoming and the outgoing information for the data patterns that are typical of an attack. It detects and blocks malicious traffic and attempts by outside users to attack the client computer. Intrusion prevention also monitors outbound traffic and prevents the spread of worms. See "Managing firewall protection" on page 413. See "Managing intrusion prevention on your client computers" on page 461.	■ The rules-based firewall engine blocks malicious threats before they can harm the computer. ■ The IPS scans network traffic and files for indications of intrusions or attempted intrusions. ■ Browser Intrusion Prevention scans for the attacks that are directed at browser vulnerabilities. ■ Universal download protection monitors all downloads from browsers and validates that the downloads are not malware.

Table 1-2 Layers of protection *(continued)*

Protection type	Description	Benefit
Proactive Threat Protection	Proactive Threat Protection uses SONAR to protect against zero-day attack vulnerabilities in your network. Zero-day attack vulnerabilities are the new vulnerabilities that are not yet publicly known. Threats that exploit these vulnerabilities can evade signature-based detection, such as spyware definitions. Zero-day attacks may be used in targeted attacks and in the propagation of malicious code. SONAR provides real-time behavioral protection by monitoring processes and threats as they execute. Application and Device Control monitors and controls the behavior of applications on client computers and manages the hardware devices that access client computers. See "Managing SONAR" on page 397. See "About application and device control" on page 479. See "Setting up application and device control" on page 482.	SONAR examines programs as they run, and identifies and stops malicious behavior of new and previously unknown threats. SONAR uses heuristics as well as reputation data to detect emerging and unknown threats. Application Control controls what applications are allowed to run or access system resources. Device Control manages the peripheral devices that users can attach to desktop computers.

The management server enforces each protection by using an associated policy that is downloaded to the client.

Figure 1-1 shows the categories of threats that each type of protection blocks.

Figure 1-1   An overview of protection layers
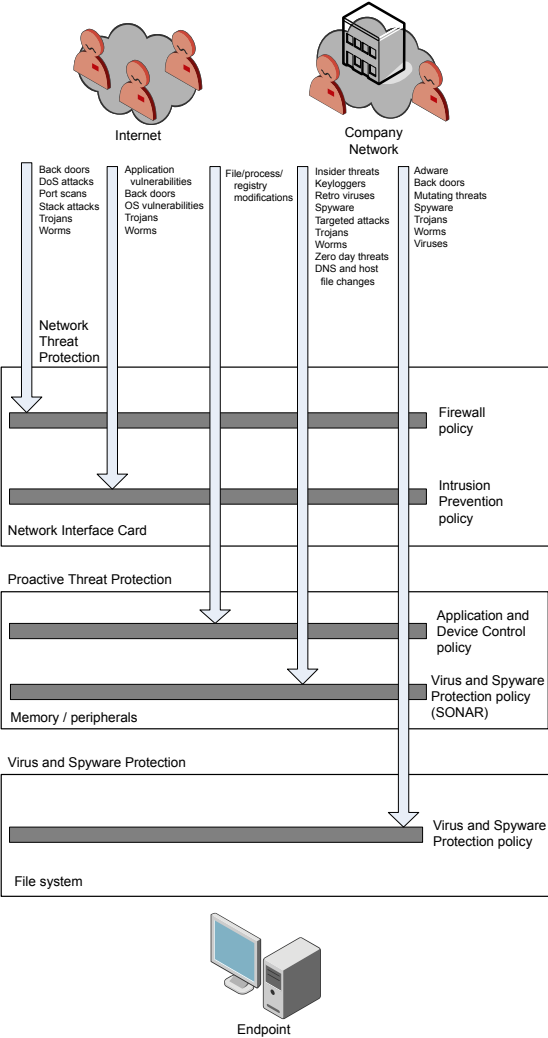
See "Components of Symantec Endpoint Protection" on page 72.

Protecting your network with Symantec Endpoint Protection

You protect the computers in your network by installing and managing the Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client.

For Symantec Network Access Control, you install Symantec Endpoint Protection Manager and the Symantec Network Access Control client.

Table 1-3 outlines the main high-level tasks that you need to do to use Symantec Endpoint Protection.

Table 1-3   Steps to set up, configure, and manage Symantec Endpoint Protection

Task	Description
Setting up Symantec Endpoint Protection	You can install Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client or Symantec Network Access Control client and protect your network in a few easy steps. See "Getting up and running on Symantec Endpoint Protection for the first time" on page 51.
Managing Symantec Endpoint Protection	Symantec Endpoint Protection Manager comes with default settings and policies so that your network is protected immediately after you install. You can modify these settings to suit your network environment. See "Managing protection on client computers" on page 60.
Maintaining a secure network environment	You might need to perform some ongoing maintenance to keep your network environment running smoothly at peak performance. For example, you must back up the database in case you need to perform disaster recovery. See "Maintaining the security of your environment" on page 62.

Table 1-3   Steps to set up, configure, and manage Symantec Endpoint
Protection *(continued)*

Task	Description
Troubleshooting Symantec Endpoint Protection and Symantec Network Access Control	If you have problems installing or using the product, Symantec Endpoint Protection Manager includes resources to help fix common issues, such as client-server communication and virus outbreaks. See "Troubleshooting Symantec Endpoint Protection" on page 64.

See "Components of Symantec Endpoint Protection" on page 72.

See the knowledge base article, Top "Best Practices" Articles for Symantec Endpoint Protection.

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

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

Table 1-4 lists the tasks that you should perform to install and protect the computers in your network immediately.

Table 1-4   Tasks to install and configure Symantec Endpoint Protection

Action	Description
Plan your network architecture	Before you install the product, perform the following tasks: ■ Make sure the computer on which you install the management server meets the minimum system requirements. For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control ■ If you install or upgrade to the Microsoft SQL Server database, make sure that you have the user name and password information. See "About SQL Server configuration settings" on page 89. ■ For networks with more than 500 clients, determine the sizing requirements. You need to evaluate several factors to ensure good network and database performance. For example, you should identify how many computers need protection and how often to schedule content updates. For more information to help you plan medium to large-scale installations, see the Symantec white paper, Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper.
Install, upgrade, or migrate the management server	Whether you install the product for the first time, upgrade from a previous version, or migrate from another product, you install Symantec Endpoint Protection Manager first. See "Installing Symantec Endpoint Protection Manager" on page 95. See "Upgrading to a new release of Symantec Endpoint Protection" on page 156. See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

Table 1-4   Tasks to install and configure Symantec Endpoint Protection
(continued)

Action	Description
Create groups and locations	You can add groups that contain computers based on the level of security or function the computers perform. For example, you should put computers with a higher level of security in one group, or a group of Mac computers in another group. You can use the following group structure as a basis: ■ Desktops ■ Laptops ■ Servers See "How you can structure groups" on page 209. See "Adding a group" on page 210. You can migrate existing Active Directory groups when you install Symantec Endpoint Protection Manager. If you are running legacy Symantec protection, you usually upgrade policy and group settings from your older version. See "Importing existing groups and computers from an Active Directory or an LDAP server" on page 211. You can apply a different level of security to computers based on whether they are inside or outside the company network. To use this method, you create separate locations and apply different security policies to each location. In general, the computers that connect to your network from outside of your firewall need to have stronger security than those that are inside your firewall. You can set up a location that allows the mobile computers that are not in the office to update their definitions automatically from Symantec's LiveUpdate servers. See "Adding a location to a group" on page 252. See "What you can do from the console" on page 105.
Disable inheritance on special groups	By default, groups inherit the security and the policy settings from the default parent group, **My Company**. You must disable inheritance before you can change the policy settings for any new groups that you create. See "Disabling and enabling a group's inheritance" on page 218.

Table 1-4	Tasks to install and configure Symantec Endpoint Protection *(continued)*

Action	Description
Change communication settings to increase performance	You can improve network performance by modifying the following client-server communication settings in each group: ■ Use pull mode instead of push mode to control when clients use network resources to download policies and content updates. ■ Increase the heartbeat interval and the randomization interval. For under 100 clients per server, increase the heartbeat to 15-30 minutes. For 100 to 1,000 clients, increase the heartbeat to 30-60 minutes. Larger environments might need a longer heartbeat interval. ■ Increase the download randomization to between one and three times the heartbeat interval. See "Randomizing content downloads from the default management server or a Group Update Provider" on page 573. See "Configuring push mode or pull mode to update client policies and content" on page 308. For more information, see the Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper.
Activate the product license	Purchase and activate a license within 60 days of product installation. See "Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license" on page 114.
Prepare computers for remote client installation (optional)	If you deploy client software remotely, first modify the firewall settings on your client computers to allow communication between the computers and the management server. See "Preparing Windows operating systems for remote deployment" on page 127. See "About firewalls and communication ports" on page 129. See "Preparing for client installation" on page 125.

Table 1-4   Tasks to install and configure Symantec Endpoint Protection
(continued)

Action	Description
Install the client software by using the Client Deployment Wizard	Create a client installation package and deploy it on your client computers. See "Deploying clients using a Web link and email" on page 132. See "Deploying clients by using Remote Push" on page 135. See "Deploying clients by using Save Package" on page 137. See "Exporting client installation packages" on page 139. Create a custom client install feature set with the following settings: ■ Use **Computer mode** for most environments, not **User mode**. See "Switching a client between user mode and computer mode" on page 234. ■ For client installation packages for workstations, check the email scanner protection option that applies to the mail server in your environment. For example, if you use a Microsoft Exchange mail server, check **Microsoft Outlook Scanner**. See "Configuring client installation package features" on page 142.

| Table 1-4 | Tasks to install and configure Symantec Endpoint Protection *(continued)* |

Action	Description

Check that the computers are listed in the groups that you expected and that the clients communicate with the management server	In the management console, on the **Clients > Clients** page:
	
	1 Change the view to **Client status** to make sure that the client computers in each group communicate with the management server.
	
	    Look at the information in the following columns:
	    ■ The **Name** column displays a green dot for the clients that are connected to the management server.
	      See "How to determine whether the client is connected in the console" on page 224.
	    ■ The **Last Time Status Changed** column displays the time that each client last communicated with the management server.
	    ■ The **Restart Required** column displays the client computers you need to restart to enable protection.
	      See "Restarting client computers" on page 145.
	    ■ The **Policy Serial Number** column displays the most current policy serial number. The policy might not update for one to two heartbeats. You can manually update the policy on the client if the policy does not update immediately.
	      See "Using the policy serial number to check client-server communication" on page 309.
	      See "Manually updating policies on the client" on page 310.
	
	2 Change to the **Protection technology** view and ensure that the status is set to **On** in the columns between and including **AntiVirus Status** and **Tamper Protection Status**.
	
	    See "Viewing the protection status of clients and client computers" on page 226.
	
	3 On the client, check that the client is connected to a server, and check that the policy serial number is the most current one.
	
	    See "Checking the connection to the management server on the client computer" on page 759.
	
	See "Troubleshooting communication problems between the management server and the client" on page 756.

Table 1-5 displays the tasks to perform after you install and configure the product to assess whether the client computers have the correct level of protection.

Table 1-5   Tasks to perform two weeks after you install

Action	Description

Modify the Virus and Spyware Protection policy	Change the following default scan settings:
	■ If you create a group for servers, change the scheduled scan time to a time when most users are offline.
	 See "Setting up scheduled scans that run on Windows computers" on page 341.
	■ Enable Risk Tracer in Auto-Protect.
	 For more information, see the Symantec Technical Support knowledge base article, What is Risk Tracer?
	 Risk Tracer has the following prerequisites:
	  ■ Network Threat Protection is enabled.
	   See "Running commands on the client computer from the console" on page 233.
	  ■ Windows File and Printer Sharing is turned on.
	 See "Customizing Auto-Protect for Windows clients" on page 378.

Modify the Firewall policy for the remote computers group and the servers group	■ Increase the security for remote computers by making sure that the following default firewall rules for an off-site location are enabled:
	  ■ **Block Local File Sharing to external computers**
	  ■ **Block Remote Administration**
	■ Decrease the security for the servers group by making sure that the following firewall rule is enabled: **Allow Local File Sharing to local computers**. This firewall rule ensures that only local traffic is allowed.
	
	See "Customizing firewall rules" on page 450.
	
	See "Managing locations for remote clients" on page 249.

	Table 1-5	Tasks to perform two weeks after you install *(continued)*

Action	Description
Exclude applications and files from being scanned	You can increase performance by configuring the client not to scan certain folders and files. For example, the client scans the mail server directory every time a scheduled scan runs. You should exclude mail server program files and directories from being scanned.
	For more information, see the knowledge base article: About the automatic exclusion of files and folders for Microsoft Exchange server and Symantec products.
	You can improve performance by excluding the folders and files that are known to cause problems if they are scanned. For example, Symantec Endpoint Protection should not scan the proprietary Microsoft SQL Server files. You should add an exception that prevents scanning of the folders that contain the Microsoft SQL Server database files. These exceptions improve performance and avoid corruption or files being locked when the Microsoft SQL Server must use them.
	For more information, see the knowledge base article: How to exclude MS SQL files and folders using Centralized Exceptions.
	You can also exclude files by extension for Auto-Protect scans on Windows computers.
	See "Creating exceptions for Symantec Endpoint Protection" on page 530.
	See "Customizing Auto-Protect for Windows clients" on page 378.
	See "Customizing Auto-Protect for Mac clients" on page 379.
Run a quick report and scheduled report after the scheduled scan	Run the quick reports and scheduled reports to see whether the client computers have the correct level of security.
	See "About the types of reports" on page 616.
	See "Running and customizing quick reports" on page 618.
	See "Creating scheduled reports" on page 621.
Check to ensure that scheduled scans have been successful and clients operate as expected	Review monitors, logs, and the status of client computers to make sure that you have the correct level of protection for each group.
	See "Monitoring endpoint protection" on page 603.

Table 1-5   Tasks to perform two weeks after you install *(continued)*

Action	Description
Configure the content revisions available to clients to reduce bandwidth	Set the number of content revisions that are stored on the management server to reduce bandwidth usage for clients. The more content revisions that the client stores, the clients are likely to download a smaller incremental package. However, you should balance bandwidth usage with the amount of hard disk space.
	■ Typically, three content updates are delivered per day. You configure the number of updates that are retained on the server. You generally want to store only the most recent content updates. A client that has not connected during the time it takes the server to accumulate the set number of updates, downloads an entire content package. An entire package is typically larger than 100 MB. An incremental update is between 1 MB and 2 MB. You configure the number of stored updates to minimize how often a client must download a complete update package.
	■ As a general rule, 1content revision uses about 1.4 GB of disk space on the Symantec Endpoint Protection Manager. When LiveUpdate for the management server is set to the default of every four hours, 10 content revisions cover at least three days.
	For more information about calculating storage and bandwidth needs, see the Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper.
Configure notifications for a single risk outbreak and when a new risk is detected	Create a notification for a **Single risk event** and modify the notification for **Risk Outbreak**.
	For these notifications, Symantec recommends that you do the following actions:
	1 Change the **Risk severity** to **Category 1 (Very Low and above)** to avoid receiving emails about tracking cookies.
	2 Keep the **Damper** setting at **Auto**.
	Notifications are critical to maintaining a secure environment and can also save you time.
	See "Setting up administrator notifications" on page 642.
	See "Managing notifications" on page 633.
Increase the time that the console leaves you logged on	The console logs you out after one hour. You can increase this period of time.
	See "Increasing the time period for staying logged on to the console" on page 105.

See "Protecting your network with Symantec Endpoint Protection" on page 50.

See the knowledge base article, Top "Best Practices" Articles for Symantec Endpoint Protection.

Managing protection on client computers

You use a single management console to manage the protection on the client computers. Although the client computers are protected immediately, you might need to modify the protection to suit your needs.

Table 1-6 outlines the tasks that you can perform if you need to adjust the default settings.

Table 1-6   Modifying protection on the client computer

Task	Description
Organizing and managing groups	You apply protection to the client computers based on the group that you place a computer in. The computers in each group have the same level of security.
	You can import your company's existing group structure. You can also create new groups.
	To determine which groups to add, first consider the structure of the network. Or, if you create a new group structure, you base your group structure on function, role, geography, or a combination of criteria. For example, consider the number of computers at the site, or whether the computers are the same type, such as Windows or Mac computers.
	See "Managing groups of clients" on page 207.
	See "Managing client computers" on page 222.
	By adding locations to a group, you can change which policy is assigned to a client computer based on where the computer is located. For example, you might want a different policy that is applied to a client computer in an office, home, or other business.
	See "Managing locations for remote clients" on page 249.
Modifying protection	Symantec Endpoint Protection Manager includes default policies for each type of protection. The policies balance the need for protection with performance. Out of the box, the default policies provide appropriate settings for large and small organizations. You may want to adjust settings over time based on your company needs.
	See "About the types of threat protection that Symantec Endpoint Protection provides" on page 46.
	See "Managing scans on client computers" on page 323.
	See "Managing firewall protection" on page 413.
	See "Managing intrusion prevention on your client computers" on page 461.
	See "Setting up application and device control" on page 482.

Table 1-6   Modifying protection on the client computer *(continued)*

Task	Description
Configuring protection in virtual environments	Symantec Endpoint Protection provides features that improve performance in virtual environments. See "Using Symantec Endpoint Protection in virtual infrastructures" on page 649.
Managing policies	Security policies must be applied to a group before the clients apply the policies to the client computer. You can create policies that all groups share or that apply to only one group. Symantec Endpoint Protection Manager makes it easy to add and modify policies for all the security needs of your company. See "The types of security policies" on page 293. See "Performing the tasks that are common to all policies" on page 290.
Scheduling and managing updates	Client computers need to receive periodic updates to protection content such as virus definitions, intrusion prevention signatures, and product software. You can configure the method, type of content, and schedule that Symantec Endpoint Protection uses to download the content to the client computers. See "Managing content updates" on page 546.
Controlling user access	You can configure the client to display different client features and protection features. How you configure these features depends on how much control you want client computer users in each group to have. See "Changing the user control level" on page 239. See "Configuring user interface settings" on page 242.
Managing client deployment	Symantec recommends that you analyze which computers need which type of security. If you did not deploy the client installation package at the time that you installed Symantec Endpoint Protection Manager, you can deploy the client software later. You have the option to look for unprotected computers. See "Preparing for client installation" on page 125. See "Deploying clients using a Web link and email" on page 132.
Monitoring and responding to status changes	You use reports and logs to view the security status of the client computers. The reports and logs help you to handle virus outbreaks and to increase the security and performance of your company's network. You can also configure notifications to alert administrators and computer users about potential security problems. See "Monitoring endpoint protection" on page 603. See "Managing notifications" on page 633.

| | Table 1-6 | Modifying protection on the client computer *(continued)* |

Task	Description
Optimizing Symantec Endpoint Protection	You can configure Symantec Endpoint Protection to improve performance on the management server and on the client computers. See "Improving client and server performance" on page 707.
Managing domains and administrators Managing administrators	Domains separate administrative duties for a set of groups. You use domains to manage the client computers that are located in different companies or business units. You can add administrator accounts so that different administrators have different levels of control over managing the groups, policies, commands, and reports in Symantec Endpoint Protection Manager. See "Managing domains and administrator accounts" on page 269.
Managing endpoint compliance	You can install and manage Symantec Network Access Control to ensure that a client computer is compliant with the company's security policy. If the computer is compliant, the computer is allowed to connect to the company network. If the client computer is not compliant, the computer must first obtain and run the software it needs to automatically remediate compliance failures before the computer can connect to the network. See "About the types of enforcement in Symantec Network Access Control" on page 780. See "Deploying Symantec Network Access Control" on page 797.

See "Protecting your network with Symantec Endpoint Protection" on page 50.

See "Getting up and running on Symantec Endpoint Protection for the first time" on page 51.

Maintaining the security of your environment

After you have secured your network, you might want to modify the protection and infrastructure to increase security or increase performance.

You might need to adapt to architectural changes, such as adding a new management server or providing protection for additional client computers.

Table 1-7   Tasks you can perform to maintain the security of your network

Task	Description
Checking the security status of your network	You should periodically check the Home page to view the overall security status of your network. You can use the notifications, reports, and logs to provide the details on the security status. See "Monitoring endpoint protection" on page 603. See "Managing notifications" on page 633.
Maintaining the database	Symantec Endpoint Protection Manager supports both the embedded database and a Microsoft SQL database. The database stores information about the settings that you configure in the management server, such as the policies, groups, client installation packages, and log entries. If bandwidth or hard disk space is an issue, you can minimize the amount of stored data and perform other tasks to increase database performance. In case of data corruption or hardware failure, you should back up the database regularly. See "Maintaining the database" on page 721.
Maintaining licenses	You can check whether your license is about to expire or if you have too many deployed clients for what your license covers. See "Licensing Symantec Endpoint Protection" on page 109.
Preparing for disaster recovery	To help mitigate a case of data corruption or a hardware failure, you should back up the database regularly and make a copy of specific management server files. See "Preparing for disaster recovery" on page 743.
Reconfiguring servers	As you add more client computers, you might need to install additional management servers and configure them. You might need to configure failover and load balancing. You might also need to switch from an embedded database to a Microsoft SQL database. See "Managing Symantec Endpoint Protection Manager servers and third-party servers" on page 715. See "Establishing communication between the management server and email servers" on page 640. See "Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server" on page 565. See "Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate" on page 564.

| Table 1-7 | Tasks you can perform to maintain the security of your network *(continued)* |

Task	Description
Setting up failover and load balancing	Within a site, you set up failover to maintain communication when clients are not able to communicate with a management server. You set up load balancing to distribute client management between management servers. See "Setting up failover and load balancing" on page 737.

See "Protecting your network with Symantec Endpoint Protection" on page 50.

Troubleshooting Symantec Endpoint Protection

Table 1-8 displays the most common issues that you might encounter when you install and use Symantec Endpoint Protection.

| Table 1-8 | Common issues you can troubleshoot |

Task	Description
Fixing installation problems	You can download and run the Symantec Endpoint Protection Support Tool to verify that your computers are ready for installation. The support tool is provided with the management server and the client. It is also available on the Symantec Support Web site. See "Troubleshooting computer issues with the Symantec Help support tool" on page 755. See "Identifying the point of failure of an installation" on page 756.
Handling virus outbreaks	You can prevent threats from attacking computers on your network. See "Preventing and handling virus and spyware attacks on client computers" on page 318. See "Remediating risks on the computers in your network" on page 320. If a threat does attack a client computer, you can identify and respond to the threat. See the following knowledge base article: Best practices for troubleshooting viruses on a network.
Troubleshooting content update problems	If the latest virus definitions do not update correctly on Symantec Endpoint Protection Manager or the clients, see the following knowledge base article: Symantec Endpoint Protection: LiveUpdate Troubleshooting Flowchart.

| Table 1-8 | Common issues you can troubleshoot *(continued)* |

Task	Description
Fixing communication errors	The communication channels between all of the Symantec Endpoint Protection components must be open. These channels include, server to client, server to database, and server and client to the content delivery component, such as LiveUpdate. See "Troubleshooting communication problems between the management server and the client" on page 756. See "Troubleshooting communication problems between the management server and the console or the database" on page 766. See the following knowledge base article: Troubleshooting Symantec Endpoint Protection Manager communication problems.
Performing disaster recovery	In case of database corruption or hardware failure, you can restore the latest snapshot of the database if you have a database backup file. See "Performing disaster recovery" on page 749.
Reducing the space in the database	You can make more space available on the database if the database size gets too large. See "Maintaining the database" on page 721.
Troubleshooting reporting issues	You can solve various report and log issues. See "Troubleshooting reporting issues" on page 771.
Troubleshooting problems with the Enforcer appliance	You can solve various Enforcer appliance problems. See "Troubleshooting an Enforcer appliance" on page 1073.

See "Protecting your network with Symantec Endpoint Protection" on page 50.

Section 1

Installing Symantec Endpoint Protection

Planning the installation

This chapter includes the following topics:

- Planning the installation
- Components of Symantec Endpoint Protection
- Components of Symantec Network Access Control
- System requirements for Symantec Endpoint Protection
- Product license requirements
- Supported virtual installations and virtualization products
- About Symantec Endpoint Protection Manager compatibility with other products
- Network architecture considerations
- About choosing a database type
- About embedded database settings
- About SQL Server configuration settings
- About SQL Server database authentication modes

Planning the installation

Table 2-1 summarizes the high-level steps to install Symantec Endpoint Protection.

	Table 2-1	Installation planning

Step	Action	Description
Step 1	Plan network architecture	Understand the sizing requirements for your network. In addition to identifying the endpoints requiring protection, scheduling updates, and other variables should be evaluated to ensure good network and database performance.
		For information to help you plan medium to large-scale installations, see the Symantec white paper: Sizing and Scalability Recommendations for Symantec Endpoint Protection
		See "Network architecture considerations" on page 85.
Step 2	Review and purchase a license	Understand the product licensing requirements. Purchase a license within 60 days of product installation.
		See "Licensing Symantec Endpoint Protection" on page 109.
		See "Product license requirements" on page 82.
Step 3	Review system requirements	Make sure that the computers on which you install the client and the management server software comply with the minimum system requirements.
		See the knowledge base article: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control
Step 4	Prepare computers for installation	To install both management server and clients, you must be logged in with an account that grants local administrator access. Uninstall other security software from your computers by configuring your Symantec Endpoint Protection client install package to automatically uninstall it. You can also manually uninstall other security software. Some programs may have special uninstallation routines. See the documentation for the third-party software.
		Make sure that administrator access to remote systems is available. Open firewalls (including ports and protocols) to allow remote deployment between the Symantec Endpoint Protection Manager and the endpoint computers.
		See "Preparing for client installation" on page 125.
		See "Configuring client packages to uninstall existing third-party security software" on page 143.
		See "Preparing Windows operating systems for remote deployment" on page 127.
		See "About firewalls and communication ports" on page 129.

<div align="center">**Table 2-1**   Installation planning *(continued)*</div>

Step	Action	Description
Step 5	Prepare to install management server	Decide on the following items before installation of the management server: ■ A password for your login to the management console ■ An email address where you can receive important notifications and reports ■ An encryption password, which may be needed depending on the options that you select during installation If you decide to use a Microsoft SQL Server database, the installation requires additional steps. These include, but are not limited to, configuring or creating a database instance that is configured to use mixed mode or Windows authentication mode. You also need to provide database server administration credentials to create the database and the database user. These are specifically for use with the management server. You need to create a password for the database user, and a user name if you do not want to accept the default. You should have this information available and configuration tasks completed before you begin installation of the management server. See "Configuring the management server during installation" on page 97. See "About embedded database settings" on page 88. See "About SQL Server configuration settings" on page 89.
Step 6	Install the management server	Install Symantec Endpoint Protection Manager. If the network that supports your business is small and located in one geographic location, you need to install only one Symantec Endpoint Protection Manager. If your network is geographically dispersed, you may need to install additional management servers for load balancing and bandwidth distribution purposes. If your network is very large, you can install additional sites with additional databases and configure them to share data with replication. To provide additional redundancy, you can install additional sites for failover or load balancing support. Failover and load balancing can only be used with Microsoft SQL Server databases. See "Setting up failover and load balancing" on page 737. See "Installing Symantec Endpoint Protection Manager" on page 95.

Table 2-1		Installation planning *(continued)*
Step	**Action**	**Description**
Step 7	Prepare and deploy client software	Determine which method would work best in your environment to deploy the client software to your computers.
		Install the Symantec Endpoint Protection client on your endpoint computers.
		Note: Symantec recommends that you also install the client on the computer that hosts Symantec Endpoint Protection Manager.
		See "About client deployment methods" on page 131.
Step 8	Post-installation tasks	Verify that your client computers are online and protected.
		Become familiar with the features and functions of the Symantec Endpoint Protection management console and perform configuration and optimization tasks.
		See "Getting up and running on Symantec Endpoint Protection for the first time" on page 51.

Components of Symantec Endpoint Protection

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

Table 2-2	Product components
Component	**Description**
Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager is a management server that manages the client computers that connect to your company's network.
	Symantec Endpoint Protection Manager includes the following components:
	■ The management server software provides secure communication to and from the client computers and the console.
	■ The console is the interface to the management server. The console software coordinates and manages security policies, client computers, reports, logs, roles and access, administrative functions, and security. You can also install a remote console and use it to log on to the management server from any computer with a network connection.
	See "What you can do from the console" on page 105.
	See "Installing Symantec Endpoint Protection Manager" on page 95.

Table 2-2   Product components *(continued)*

Component	Description
Database	The database stores security policies and events. You install the embedded database on the computer that hosts Symantec Endpoint Protection Manager.
	You can also separately install the Microsoft SQL Server database to use instead of the embedded database.
	See "About choosing a database type" on page 87.
Symantec Endpoint Protection client	The client protects computers with virus and spyware scans, SONAR, Download Insight, a firewall, an intrusion prevention system, and other protection technologies. It runs on the servers, desktops, and portable computers that you want to protect.
	The Symantec Endpoint Protection Mac client protects the computers with virus and spyware scans.
	For more information about using the client, see the *Symantec Endpoint Protection and Symantec Network Access Control Client Guide*.
	See "About Symantec Endpoint Protection" on page 41.
Symantec Protection Center (optional)	Symantec Protection Center lets you integrate management consoles from multiple supported Symantec security products into a single management environment. Symantec Endpoint Protection integrates with Protection Center by means of a series of Web services.
	You download and install Protection Center version 2 separately.
	See "About Symantec Endpoint Protection and Protection Center" on page 199.
	See the Symantec Protection Center 2.0 Getting Started Guide
LiveUpdate Administrator (optional)	The LiveUpdate Administrator downloads definitions, signatures, and product updates from a Symantec LiveUpdate server and distributes the updates to client computers.
	For more information, see the *Symantec LiveUpdate Administrator User's Guide*.
Central Quarantine (optional)	The Central Quarantine receives suspicious files and unrepaired infected items from the Symantec Endpoint Protection clients. Central Quarantine forwards a sample to Symantec Security Response, which analyzes the sample. If a threat is new, Symantec Security Response produces security updates.
	For more information, see the *Symantec Central Quarantine Implementation Guide*.

See "Components of Symantec Network Access Control" on page 74.

See "About the types of threat protection that Symantec Endpoint Protection provides" on page 46.

Components of Symantec Network Access Control

Table 2-3 lists the product's components and describes their functions.

Table 2-3   Symantec Network Access Control product components

Component	Description
Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager is a management server that manages the client computers that connect to your company's network.
	Symantec Endpoint Protection Manager includes the following software:
	■ The management server software provides secure communication to and from the client computers and the console.
	■ The console is the interface to the management server. The console software coordinates and manages security policies, client computers, reports, logs, roles and access, administrative functions, and security. You can also install a remote console and use it to log on to the management server from any computer with a network connection.
	See "What you can do from the console" on page 105.
	See "Installing Symantec Endpoint Protection Manager" on page 95.
Database	The database stores security policies and events. You install the embedded database on the computer that hosts Symantec Endpoint Protection Manager.
	You can also separately install the Microsoft SQL Server database to use instead of the embedded database.
	See "About choosing a database type" on page 87.
Symantec Network Access Control client	The Symantec Network Access Control client enforces security policy compliance on the client computers by using Host Integrity checks and self-enforcement capabilities. The client reports its Host Integrity compliance status to a Symantec Enforcer.
	For more information about using the client, see the *Symantec Endpoint Protection and Symantec Network Access Control Client Guide*.
	See "About Symantec Network Access Control" on page 780.
Symantec Protection Center	Symantec Protection Center lets you integrate management consoles from multiple supported Symantec security products into a single management environment. Symantec Endpoint Protection integrates with Protection Center by means of a series of Web services.
	You download and install Protection Center version 2 separately.
	See "About Symantec Endpoint Protection and Protection Center" on page 199.

	Table 2-3	Symantec Network Access Control product components *(continued)*

Component	Description
LiveUpdate Administrator (optional)	The LiveUpdate Administrator downloads definitions, signatures, and product updates from a Symantec LiveUpdate server and distributes the updates to client computers. For more information, see the *Symantec LiveUpdate Administrator User's Guide*.
Symantec Enforcer (optional)	An Enforcer ensures that the clients that try to connect to the network comply with configured security policies. You can restrict non-compliant computers to specific network segments for remediation and you can completely prohibit access to non-compliant computers. Symantec Network Access Control includes the following types of Enforcers: ■ The Gateway Enforcer appliance provides in-line enforcement at network choke points. ■ The LAN 802.1X Enforcer appliance provides an out-of-band standards-based approach for LAN and wireless networks. ■ The DHCP Integrated Enforcer provides a DHCP-based approach for LAN and wireless networks over any infrastructure. ■ The Microsoft Network Access Protection Integrated Enforcer provides a Microsoft NAP-based approach for LAN and wireless networks. See About the LAN Enforcer appliance installation on page 785. See "About the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers" on page 983. See "About the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection" on page 984.
Symantec Network Access Control On-Demand clients for Windows and Mac (optional)	On-demand clients are the temporary clients that you provide to users when they are unauthorized to access your network. Unauthorized client computers do not have the software that is compliant with your security policy. Once the Enforcer has installed an on-demand client, it temporarily connects to your enterprise network as a guest. See "About the Symantec Network Access Control On-Demand Clients" on page 1048.

System requirements for Symantec Endpoint Protection

In general, the system requirements for Symantec Endpoint Protection Manager and the clients are the same as those of the supported operating systems.

Table 2-4 displays the minimum requirements for the Symantec Endpoint Protection Manager.

Table 2-5 displays the minimum requirements for the Symantec Endpoint Protection client.

Table 2-6 displays the minimum requirements for the Symantec Network Access Control client.

Table 2-7 displays the minimum requirements for the Symantec Network Access Control On-Demand client.

Table 2-4　　　　Symantec Endpoint Protection Manager system requirements

Component	Requirements
Processor	■ 32-bit processor: 1-GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended) ■ 64-bit processor: 2-GHz Pentium 4 with x86-64 support or equivalent minimum **Note:** Intel Itanium IA-64 processors are not supported.
Physical RAM	1 GB of RAM for 32-bit operating systems, 2 GB of RAM for 64-bit operating systems, or higher if required by the operating system
Hard drive	4 GB or more free space; plus 4 GB for the locally installed database.
Display	800 x 600
Operating system	■ Windows XP (32-bit, SP2 or later; 64-bit, all SPs; all editions except Home) ■ Windows 7 (32-bit, 64-bit; RTM and SP1; all editions except Home) ■ Windows 8 (32-bit, 64-bit) ■ Windows Server 2003 (32-bit, 64-bit, R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit, R2, RTM, SP1 and SP2) ■ Windows Server 2012 ■ Windows Small Business Server 2003 (32-bit) ■ Windows Small Business Server 2008 (64-bit) ■ Windows Small Business Server 2011 (64-bit) ■ Windows Essential Business Server 2008 (64-bit)
Web browser	■ Microsoft Internet Explorer 7, 8, 9, 10 ■ Mozilla Firefox ■ Google Chrome

Note: This version of the Symantec Endpoint Protection Manager can manage clients before version 12.1, regardless of the client operating system.

The Symantec Endpoint Protection Manager includes an embedded database. You may also choose to use one of the following versions of Microsoft SQL Server:

■ SQL Server 2005, SP4

■ SQL Server 2008

■ SQL Server 2008 R2

■ SQL Server 2012

Note: If you install the Symantec Endpoint Protection Manager and the SQL database on the same computer, a minimum of 4 GB of RAM is recommended.

Table 2-5 Symantec Endpoint Protection Windows and Mac client system requirements

Component	Requirements
Processor	■ 32-bit processor for Windows: 1-GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended) ■ 32-bit processor for Mac: Intel Core Solo, Intel Core Duo. PowerPC processors are not supported. ■ 64-bit processor for Windows: 2-GHz Pentium 4 with x86-64 support or equivalent minimum. Itanium processors are not supported. ■ 64-bit processor for Mac: Intel Core 2 Duo, Intel Quad-Core Xeon
Physical RAM	Windows: 512 MB of RAM (1 GB recommended), or higher if required by the operating system Mac: 1 GB of RAM for 10.6; 2 GB for 10.7 and 10.8
Hard drive	Windows: 850 MB of available hard disk space for the installation; additional space is required for content and logs **Note:** Space requirements are based on NTFS file systems. Mac: 500 MB of available hard disk space for the installation
Display	800 x 600

Table 2-5   Symantec Endpoint Protection Windows and Mac client system
                    requirements *(continued)*

Component	Requirements
Operating system	■ Windows XP Home or Professional (32-bit, SP2 or later; 64-bit, all SPs) ■ Windows XP Embedded (SP2 and later) ■ Windows Vista (32-bit, 64-bit) ■ Windows 7 (32-bit, 64-bit, RTM, and SP1) ■ Windows Embedded Standard 7 ■ Windows 8 (32-bit, 64-bit) ■ Windows Server 2003 (32-bit, 64-bit, R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit, R2, SP1, and SP2) ■ Windows Server 2012 ■ Windows Small Business Server 2003 (32-bit) ■ Windows Small Business Server 2008 (64-bit) ■ Windows Small Business Server 2011 (64-bit) ■ Windows Essential Business Server 2008 (64-bit) ■ Mac OS X 10.6.8, 10.7 (32-bit, 64-bit); 10.8 (64-bit) ■ Mac OS X Server 10.6.8, 10.7 (32-bit, 64-bit); 10.8 (64-bit)

For information about the system requirements for the Symantec AntiVirus client
on Linux, see the *Symantec AntiVirus for Linux Implementation Guide*.

Table 2-6   Symantec Network Access Control client system requirements

Component	Requirement
Processor	■ 32-bit processor for Windows: 1-GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended) ■ 64-bit processor for Windows: 2-GHz Pentium 4 with x86-64 support or equivalent minimum. Itanium processors are not supported.

Table 2-6   Symantec Network Access Control client system requirements
(continued)

Component	Requirement
Operating system	■ Windows XP (32-bit, SP2 or later; 64-bit, all SPs) ■ Windows XP Embedded ■ Windows Vista (32-bit, 64-bit) ■ Windows 7 (32-bit, 64-bit) ■ Windows 8 (32-bit, 64-bit) ■ Windows Server 2003 (32-bit, 64-bit, R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit) ■ Windows Server 2012 ■ Windows Small Business Server 2008 (64-bit) ■ Windows Essential Business Server 2008 (64-bit)
Physical RAM	512 MB of RAM, or higher if required by the operating system
Hard disk	32-bit: 300 MB; 64-bit: 400 MB
Display	800 x 600

Table 2-7   Symantec Network Access Control On-Demand client system
requirements

Component	Requirement
Processor	■ Windows: Intel Pentium II 550 MHz (1 GHz for Windows Vista) or faster ■ Mac: Intel CPU only
Operating system	■ Windows XP Home or Professional (32-bit, SP2 and SP3) ■ Windows Vista (32-bit, 64-bit) ■ Windows 7 (32-bit, 64-bit) ■ Windows 8 (32-bit, 64-bit) ■ Windows Server 2003 (32-bit, 64-bit, R2, SP1 or later) ■ Windows Server 2008 (32-bit, 64-bit, R2) ■ Windows Server 2012 ■ Windows Small Business Server 2008 (64-bit) ■ Windows Essential Business Server 2008 (64-bit) ■ Mac OS X 10.5, 10.6 or 10.7

Table 2-7 Symantec Network Access Control On-Demand client system
requirements *(continued)*

Component	Requirement
Disk space and physical RAM	■ Download size: 9 MB. The amount of free disk space that is needed to run the client: 100 MB. ■ Physical RAM for either Windows or Mac On-Demand Client: 512 MB
Web browser	■ For Windows On-Demand Client: Microsoft Internet Explorer 6.0 or later; Mozilla Firefox 2.0, 3.0, 3.5, 3.6.3, 11.0 **Note:** Clients from version 11.0 RU6 and lower do not support Firefox 3.6.3. ■ For Mac On-Demand Client : Apple Safari 4.0 and 5.0; Mozilla Firefox 2.0, 3.0, 3.5, 3.6.3 **Note:** Clients from version 11.0 RU6 and lower do not support Firefox 3.6.3.
Other	■ Video display: Super VGA (1,024 x 768) or higher ■ At least one Ethernet adapter (with TCP/IP installed)

For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

See "Planning the installation" on page 69.

See "Supported virtual installations and virtualization products" on page 83.

See "Internationalization requirements" on page 80.

Internationalization requirements

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

Table 2-8   Internationalization requirements

Component	Requirements
Computer names, server names, and work group names	Non-English characters are supported with the following limitations: ■ Network audit may not work for a host or user that uses a double-byte character set or a high-ASCII character set. ■ Double-byte character set names or high-ASCII character set names may not appear properly on the Symantec Endpoint Protection Manager console or on the client user interface. ■ A long double-byte or high-ASCII character set host name cannot be longer than what NetBIOS allows. If the host name is longer than what NetBIOS allows, the Home, Monitors, and Reports pages do not appear on the Symantec Endpoint Protection Manager console.
English characters	English characters are required in the following situations: ■ Deploy a client package to a remote computer. ■ Define the server data folder in the Management Server Configuration Wizard. ■ Define the installation path for Symantec Endpoint Protection Manager. ■ Define the credentials when you deploy the client to a remote computer. ■ Define a group name. You can create a client package for a group name that contains non-English characters. You might not be able to deploy the client package using the Push Deployment Wizard when the group name contains non-English characters. ■ Push non-English characters to the client computers. Some non-English characters that are generated on the server side may not appear properly on the client user interface. For example, a double-byte character set location name does not appear properly on non-double-byte character set named client computers.
User Information client computer dialog box	Do not use double-byte or high-ASCII characters when providing feedback in the **User Information** client computer dialog box after you install the exported package. See "Collecting user information" on page 244.
License Activation wizard	Do not use double-byte characters in the following fields: ■ **First name** ■ **Last name** ■ **Company name** ■ **City** ■ **State/province** See "Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license" on page 114.

For the most current system requirements, see: Release Notes and System
Requirements for all versions of Symantec Endpoint Protection and Symantec
Network Access Control

Product license requirements

If you want to use Symantec Endpoint Protection after the trial period expires,
you must purchase then activate a product license.

Table 2-9 displays the requirements you need to license Symantec Endpoint
Protection.

Table 2-9   Product license requirements

Product	Requirement
Paid license installation of Symantec Endpoint Protection	You must purchase a license that covers each deployed client. One license covers all clients regardless of platform and version. See "About the licensing enforcement rules" on page 120.
Symantec legacy virus protection software	Symantec Endpoint Protection accepts the license file from your Symantec legacy virus protection software. You must purchase a new license when the legacy license expires.
Trialware	A 60-day trial license is included with Symantec Endpoint Protection. You must purchase a license when the trial license expires.

The following terminology applies to Symantec product licenses:

Serial number	A license contains a serial number that uniquely identifies your license and associates the license with your company. The serial number can be used to activate your Symantec Endpoint Protection license. See "Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license" on page 114.
Deployed	Deployed refers to the endpoint computers that are under the protection of the Symantec Endpoint Protection client software. For example, "We have 50 deployed seats." means that 50 endpoints have client software installed on them.

Activate	You activate your Symantec Endpoint Protection product license to enable unrestricted access to all program functionality. You use the License Activation wizard to complete the activation process.
	See "Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license" on page 114.
Seat	A seat is a single endpoint computer that the Symantec Endpoint Protection client software protects. A license is purchased and is valid for a specific number of seats. "Valid seats" refers to the total number of seats that are specified in all of your active licenses.
Trialware	Trialware refers to a fully functioning installation of Symantec Endpoint Protection operating within the free trial period. The trial period is 60 days from the initial installation of the Symantec Endpoint Protection Manager. If you want to continue using Symantec Endpoint Protection beyond the trial period, you must purchase and activate a license for your installation. You do not need to uninstall the software to convert from trialware to a licensed installation.
	See "About purchasing licenses" on page 112.
Over-deployed	A license is over-deployed when the number of deployed clients exceeds the number of licensed seats.

Understanding license requirements is part of planning your Symantec Endpoint Protection installation and after installation, managing your product licenses.

See "Planning the installation" on page 69.

See "Licensing Symantec Endpoint Protection" on page 109.

See "About purchasing licenses" on page 112.

See "Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license" on page 114.

Supported virtual installations and virtualization products

You can use the Symantec Endpoint Protection clients to protect virtual instances of the supported operating systems. You can install and manage Symantec Endpoint Protection Manager on virtual instances of the supported operating systems.

Table 2-10 lists the supported virtualization products.

Table 2-10   Supported virtualization products

Symantec software	Virtualization product
Symantec Endpoint Protection Manager, console, and embedded database components	■ VMware WS 5.0 (workstation) or later ■ VMware GSX 3.2 (enterprise) or later ■ VMware ESX 2.5 (workstation) or later ■ VMware VMotion ■ Microsoft Virtual Server 2005 ■ Windows Server 2008 Hyper-V ■ Windows 8 Server Hyper-V ■ Novell Xen ■ Virtual Box, supplied by Oracle
Symantec Endpoint Protection client software	■ VMware WS 5.0 (workstation) or later ■ VMware GSX 3.2 (enterprise) or later ■ VMware ESX 2.5 (workstation) or later ■ VMware VMotion ■ Microsoft Virtual Server 2005 ■ Windows Server 2008 Hyper-V ■ Windows 8 Server Hyper-V ■ Novell Xen ■ Virtual Box, supplied by Oracle

Symantec Endpoint Protection includes features that enhance performance in virtual environments.

See "Using Symantec Endpoint Protection in virtual infrastructures" on page 649.

See "Randomizing scans to improve computer performance in virtualized environments" on page 384.

For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

About Symantec Endpoint Protection Manager compatibility with other products

Some products may cause conflicts with Symantec Endpoint Protection when they are installed on the same server. You need to configure the Symantec Endpoint

Protection Manager installation if one or more of the following products is installed on the same server:

■ Symantec Backup Exec 10, 10D, or 11D

■ Symantec Brightmail

■ Symantec Enterprise Vault

■ Symantec Ghost Solution Suite 2.0

■ Symantec Mail Security for Exchange

■ Symantec NetBackup

■ Microsoft Outlook Web Access

■ Microsoft SharePoint

■ Microsoft Windows Update Services

In most cases, port changes are required to allow these programs to run concurrently with Symantec Endpoint Protection.

For information about the configuration changes, see the Symantec Support knowledge base article, Addressing Symantec Endpoint Protection compatibility issues.

For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

Network architecture considerations

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

See "Planning the installation" on page 69.

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

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

■ Symantec Endpoint Protection Manager
Administrators use Symantec Endpoint Protection Manager to manage security policies and client computers. You may want to consider the security and availability of the computer on which Symantec Endpoint Protection Manager is installed.

- Remote console
  Administrators can use a remote computer that runs the console software to access Symantec Endpoint Protection Manager. Administrators may use a remote computer when they are away from the office. You should ensure that remote computers meet the remote console requirements.

- Local and remote computers
  Remote computers may have slower network connections. You may want to use a different installation method than the one you use to install to local computers.

- Portable computers such as notebook computers
  Portable computers may not connect to the network on a regular schedule. You may want to make sure that portable computers have a LiveUpdate policy that enables a LiveUpdate schedule. Any portable computers that do not check in regularly do not get other policy updates.

- Computers that are located in secure areas
  Computers that are located in secure areas may need different security settings from the computers that are not located in secure areas.

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

You decide how you want to manage the computers. In most cases, you manage the computers from the Symantec Endpoint Protection Manager console. These are called "managed computers." You might want to manually manage the portable computers that connect to the company network intermittently, such as mobile devices like notebook computers. A manually-managed computer is called an "unmanaged computer." Computers that never connect to the company network are unmanaged computers by definition, because they never connect to the Symantec Endpoint Protection Manager.

You organize the computers with similar security needs into groups. For example, you might organize the computers in the Payroll department into the Payroll group. You might define the group structure to match the structure of your organization.

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

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

About choosing a database type

Symantec Endpoint Protection Manager uses a database to store information about clients and settings. The database is created as part of the configuration process. You must decide which database to use before you install the management server. You cannot use the console until you have configured the management server to use a database.

Table 2-11   Databases that Symantec Endpoint Protection Manager uses

Database type	Description
Embedded database	The embedded database is included with Symantec Endpoint Protection Manager. The embedded database does not require configuration and is easier to install. The embedded database supports up to 5,000 clients.
	See "About embedded database settings" on page 88.
Microsoft SQL Server database	If you choose to use this option, you must install Microsoft SQL Server before you install the Symantec Endpoint Protection Manager. Additionally, the SQL Server client tools must be installed on the same computer where you install Symantec Endpoint Protection Manager.
	You should consider purchasing and installing Microsoft SQL Server for the following reasons:
	■ You must support more than 5,000 clients. Each management server that uses Microsoft SQL Server can support up to 50,000 clients. If your organization has more than 50,000 clients, you can install another management server.
	■ You want to support failover and load balancing.
	■ You want to set up additional management servers as Site Partners. See "About determining how many sites you need" on page 189.
	If you create a Microsoft SQL Server database, you must first install an instance of Microsoft SQL Server. You must then configure it for communication with the management server.
	See "About SQL Server configuration settings" on page 89.

About embedded database settings

The following values represent the default settings when you install the Symantec Endpoint Protection Manager. The ports that are listed are TCP ports.

You can configure some of the following values only when you install the Symantec Endpoint Protection Manager using a custom configuration.

See "Installing Symantec Endpoint Protection Manager" on page 95.

Table 2-12   Embedded database settings

Setting	Default	Description
Server name	*local host name*	The name of the computer that runs the Symantec Endpoint Protection Manager.
Server port	8443	The Symantec Endpoint Protection Manager listens on this port.
Web console port	9090	Remote HTTP console connections use this port.
Client communications port	8014	The clients communicate with the management server on this port. Optional Enforcer hardware devices also use this port.
Protection center web services port	8444	The port over which the Symantec Protection Center 2.x makes Data Feed and Workflow requests to Symantec Endpoint Protection Manager.
Remote management web services port	8446	Remote Monitoring and Management (RMM) uses this port to send web services traffic over HTTPS.
Server control port	8765	The Tomcat web service uses this port.
Reporting port	8445	The Apache web service uses this port for reporting.
Server data folder	C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data (32-bit operating system) C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data (64-bit operating system)	The directory in which the Symantec Endpoint Protection Manager places data files including backups, replicated logs, and other files. The installer creates this directory if it does not exist.

Table 2-12   Embedded database settings *(continued)*

Setting	Default	Description
Encryption password	None	This password encrypts communication between the Symantec Endpoint Protection Manager, clients, and optional Enforcer hardware devices.
		If you choose the default configuration, the system automatically generates the encryption password for you. From the summary screen, you can print or copy this information to the clipboard.
		If you choose a custom configuration, you can have the system automatically generate a random password, or you can create your own password. The password can be from 6-32 alphanumeric characters.
		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.
		See "Preparing for disaster recovery" on page 743.
User name	admin	The name of the default user that is used to log on to the Symantec Endpoint Protection Manager console for the first time. This value is not configurable.
Password	None	The password that is specified for the admin account during server configuration.
		If the embedded database is used, the original admin password is needed to reconfigure the management server. Document this password and put it in a secure location.
Email address	None	System notifications are sent to the email address specified.

About SQL Server configuration settings

If you install Symantec Endpoint Protection Manager with a Microsoft SQL Server database, there are specific configuration requirements for SQL Server.

See "Installing Symantec Endpoint Protection Manager" on page 95.

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 existing instance, but the instance

must be configured properly or your database installation fails. For example, 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. To maximize the security posture of remote Microsoft SQL Server communications, collocate both servers in a secure subnet.

Table 2-13   Required SQL Server configuration settings

Configuration setting	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 name is supported, but can cause confusion if you install multiple instances on one computer.
Authentication configuration	Mixed Mode or Windows Authentication mode
	See "About SQL Server database authentication modes" on page 93.
sa password	Set this password when you set Mixed Mode authentication.
Enabled protocol	TCP/IP
IP addresses for TCP/IP	Enable IP1 and IP2
TCP/IP port numbers for IP1, IP2, and IPALL	Set TCP Dynamic Ports to blank, and specify a TCP Port number. The default port is typically 1433. You specify this port number when you create the database.
	The Symantec Endpoint Protection Manager database does not support dynamic ports.
Remote connections	Must be enabled. TCP/IP protocol must also be specified.

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

Endpoint Protection Manager. Refer to Microsoft SQL Server documentation for installation instructions.

During the Symantec Endpoint Protection Manager database configuration phase of the installation, you select and enter various database values. Understand the decisions you must make to correctly configure the database.

Table 2-14 displays the settings that you might need to know before you begin the installation process.

Table 2-14   SQL Server database settings

Setting	Default	Description
Server name	*local host name*	Name of the computer that runs the Symantec Endpoint Protection Manager.
Server data folder	C:\Program Files\Symantec Endpoint Protection Manager\data	Folder in which the Symantec Endpoint Protection Manager places data files including backups, replication, and other Symantec Endpoint Protection Manager files. The installer creates this folder if it does not exist.
Encryption password	None	The password that encrypts communication between the Symantec Endpoint Protection Manager, clients, and optional Enforcer hardware devices. The password can be from 6-32 alphanumeric characters and is required.
		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.
		See "Performing disaster recovery" on page 749.
Database server	*local host name*	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 *host name* or the host's *IP address*. If the database server was installed with a named instance, type either *host name\instance_name* or *IP address\instance_name*. Using *host name* 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	The port used to send and receive traffic to the SQL Server.
		Port 0, which is used to specify a random, negotiated port, is not supported.

Table 2-14   SQL Server database settings *(continued)*

Setting	Default	Description
Database Name	sem5	Name of the database that is created.
Database user name	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.
Database password	None	The password that is associated 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 Server client folder	SQL Server 2005: C:\Program Files\Microsoft SQL Server\90\Tools\Binn SQL Server 2008: C:\Program Files\Microsoft SQL Server\100\Tools\Binn SQL Server 2012 C:\Program Files\Microsoft SQL Server\110\Tools\Binn	Location of the local SQL Client Utility directory that contains bcp.exe.
Server user name	None	Name of the database server administrator account, which is typically sa.
Server password	None	The password that is associated with the database server administrator account.

Table 2-14   SQL Server database settings *(continued)*

Setting	Default	Description
Database data folder	Automatically detected after clicking Default. SQL Server 2005: C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data SQL Server 2008: C:\Program Files\Microsoft SQL Server\ MSSQL10.MSSQLSERVER\ MSSQL\Data SQL Server 2008 R2: C:\ Program Files\Microsoft SQL Server\ MSSQL10_50.MSSQLSERVER\ MSSQL\Data SQL Server 2012: C:\Program Files\Microsoft SQL Server\ MSSQL11.MSSQLSERVER\ MSSQL\Data	Location of the SQL Server data folder. If you install to a remote server, the volume identifier must match the identifier on the remote server. ■ If you install to a named instance on SQL Server 2005, the instance name is appended to MSSQL with a dot numeric identifier. For example, \MSSQL.*n*\MSSQL\Data ■ If you install to a named instance on SQL Server 2008, the instance name is appended to MSSQL10. For example, \MSSQL10.*instance name*\MSSQL\Data. ■ If you install to a named instance on SQL Server 2008 R2, the instance name is appended to MSSQL10_50. For example, \MSSQL10_50.*instance name*\MSSQL\Data. ■ If you install to a named instance on SQL Server 2012, the instance name is appended to MSSQL11. For example, \MSSQL11.*instance name*\MSSQL\Data. **Note:** Clicking Default displays the correct installation folder, if you entered the database server and instance name correctly. If you click Default and the correct installation folder does not appear, your database creation fails.

About SQL Server database authentication modes

The Symantec Endpoint Protection Manager supports two modes of SQL Server database authentication:

■ Windows Authentication mode

■ Mixed mode

Microsoft SQL Server can be configured to use either Windows Authentication or Mixed mode authentication. Mixed mode authentication allows the use of either Windows or SQL Server credentials. When SQL Server is configured to use Mixed mode, Symantec Endpoint Protection Manager may be set to use either Windows Authentication or Mixed mode authentication. When SQL Server is set to use Windows Authentication mode, Symantec Endpoint Protection Manager must also be configured to use Windows Authentication mode.

For the remote database connections that use the Windows Authentication mode, be aware of the following requirements:

■ For deployments in an Active Directory environment, the Symantec Endpoint Protection Manager and SQL Server must be located in the same Windows domain.

■ For deployments in a Workgroup environment, the Windows account credentials must be the same for the local computers and the remote computers.

See "About SQL Server configuration settings" on page 89.

Installing Symantec Endpoint Protection Manager

This chapter includes the following topics:

- Installing Symantec Endpoint Protection Manager
- Configuring the management server during installation
- Uninstalling Symantec Endpoint Protection Manager
- About accepting the self-signed (SSL) server certificate for Symantec Endpoint Protection Manager
- Logging on to the Symantec Endpoint Protection Manager console
- Increasing the time period for staying logged on to the console
- What you can do from the console

Installing Symantec Endpoint Protection Manager

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

Note: The Symantec Endpoint Protection Manager requires access to the system registry for installation and normal operation. To prepare a server that runs Windows Server 2003 to install Symantec Endpoint Protection Manager using a remote desktop connection, you must first allow remote control on the server. You must also use a remote console session, or shadow the console session.

For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

See "Preparing for client installation" on page 125.

See "Getting up and running on Symantec Endpoint Protection for the first time" on page 51.

To install Symantec Endpoint Protection Manager

1   Insert and display the product disc.

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

    If you downloaded the product, extract the entire product disc image to a physical disc, such as a hard disk. Run **Setup.exe** from the physical disc.

2   In the **Symantec Endpoint Protection Installation Program** dialog box, click **Install Symantec Endpoint Protection**, and then click **Install Symantec Endpoint Protection Manager**.

3   Review the sequence of installation events, and then click **Next** to begin.

4   In the **License Agreement** panel, click **I accept the terms in the license agreement**, and then click **Next**.

5   In the **Destination Folder** panel, accept the default destination folder or specify another destination folder, and then click **Next**.

6   Click **Install**.

    The installation process begins for the Symantec Endpoint Protection Manager and console. When the installation is complete, click **Next**.

7   After the initial installation completes, you configure the server and database. Click **Next**.

    The **Management Server Configuration Wizard** starts.

    See "Configuring the management server during installation" on page 97.

    See "About choosing a database type" on page 87.

8   You configure the management server according to your requirements. Follow
    the on-screen instructions. After the server and the database configuration,
    click **Next** to create the database.

9   Click **Finish** to complete the configuration.

    The Symantec Endpoint Protection Manager console log on screen appears
    if you leave the option checked. Once you log in, you can begin client
    deployment. You can also optionally run the Migration Wizard at this time,
    if desired.

    See "About client deployment methods" on page 131.

    See "Deploying clients using a Web link and email" on page 132.

    See "Migrating from Symantec AntiVirus or Symantec Client Security"
    on page 177.

Configuring the management server during installation

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

See "Installing Symantec Endpoint Protection Manager" on page 95.

You can also start the Management Server Configuration Wizard at any time after
installation from **Start > All Programs > Symantec Endpoint Protection Manager
> Symantec Endpoint Protection Manager Tools**.

To configure the server, you specify the following information:

■   The configuration type: default or custom. The wizard provides information
    about each type.

■   Whether you want to use a recovery file.

Note: If this is your first installation of Symantec Endpoint Protection Manager,
there is no recovery file.

See "Performing disaster recovery" on page 749.

■   The password for the default administrator account.

■   The email address that receives important notifications and reports.

■   The email server name and port number.

■ You can optionally add partner information if you have a Symantec Sales Partner who manages your Symantec licenses.

Each configuration type has a separate configuration process. Follow the instructions that are provided in the Management Server Configuration Wizard to complete the configuration.

See "Planning the installation" on page 69.

Uninstalling Symantec Endpoint Protection Manager

Uninstalling Symantec Endpoint Protection Manager uninstalls the server and console. You can optionally remove the database and the database backup files during uninstallation.

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

You must turn off replication before you attempt to uninstall a Symantec Endpoint Protection Manager that is set up for replication.

To uninstall Symantec Endpoint Protection Manager

The text that you see depends on the operating system of the server computer.

1   On the server computer, on the **Start** menu, click **Control Panel** > **Add or Remove Programs** (or **Control Panel > Programs** > **Uninstall a program**).

2   In the **Add or Remove Programs** (or **Uninstall or change a program**) dialog box, click **Symantec Endpoint Protection Manager**, and then click **Change**, **Remove**, or **Uninstall**.

3   Follow the onscreen prompts to remove Symantec Endpoint Protection Manager.

In some cases, you may have to uninstall Symantec Endpoint Protection Manager manually.

For more information, see the knowledge base article: Methods for uninstalling Symantec Endpoint Protection.

See "Backing up the database and logs" on page 744.

See "Turning off replication before upgrade" on page 168.

See "Turning on replication after upgrade" on page 169.

About accepting the self-signed (SSL) server certificate for Symantec Endpoint Protection Manager

When you install Symantec Endpoint Protection Manager, a self-signed certificate for the pages that are rendered in a browser is included as part of the installation. When you first access these pages from a remote console, you must accept the self-signed certificate for the pages to display.

The certificates are stored separately for each user. Each administrator account must accept the certificate for each remote location from which they connect to the management server.

For instructions to add the security certificate to the Web browser, see the Symantec Technical Support knowledge base article, How to install the certificate for Symantec Protection Center or Endpoint Protection Manager for Web console access.

See "Logging on to the Symantec Endpoint Protection Manager console" on page 99.

Logging on to the Symantec Endpoint Protection Manager console

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

- Locally, from the computer on which the management server is installed.

- Remotely, from any computer that meets the system requirements for a remote console and has network connectivity to the management server.
  You can log on to the remote Web console or the remote Java console.

To log on remotely, you need to know the IP address or the host name of the computer on which the management server is installed. You should also ensure that your Web browser Internet options let you view content from the server you log on to.

When you log on remotely, you can perform the same tasks as administrators who log on locally. What you can view and do from the console depends on the type of administrator you are. Most administrators in smaller organizations log on as a system administrator.

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

Note: If you installed the remote Java console with an earlier version of the product, you must reinstall it when you upgrade to a later version.

The console logs you out after one hour. You can increase this period of time.

To log on to the console locally

1 Go to **Start > Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager**.

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

If the console has more than one domain, click **Options >** and type the domain name.

3 Click **Log on**.

To log on to the console remotely

1 Open a supported Web browser and type the following address in the address box:

http://*host name*:9090

where *host name* is the host name or IP address of the management server. For a list of supported Web browsers, see the Knowledge Base document Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control.

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

If you click **Symantec Endpoint Protection Manager Web Console**, a secure webpage loads so you log on remotely without the use of the Java Runtime Environment (JRE).

If you click **Symantec Endpoint Protection Manager Console**, the computer from which you log on must have the JRE installed to run the Java client. If it does not, you must download and install it. Follow the prompts to install the JRE, and follow any other instructions provided.

The two other options are not remote management solutions. The option **Symantec Protection Center** directs you to the logon screen for Symantec Protection Center 1.0.0, which provides limited reporting data. See the context-sensitive help for more information. The option **Symantec Endpoint Protection Manager Certificate** prompts you to download the management console's certificate file. You can then import this file into your Web browser if needed.

3 If a host name message appears, click **Yes**.

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

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

4 Follow the prompts to complete the logon process.

Depending on the logon method, you may need to provide additional information. For instance, if the console has multiple domains, click **Options** and provide the name of the domain to which you want to log on.

When you log on for the first time after installation, use the account name **admin**.

5 Click **Log On**.

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

You may need to accept the self-signed certificate that the Symantec Endpoint Protection Manager requires.

See "Logging on to reporting from a stand-alone Web browser" on page 614.

See "Granting or blocking access to remote Symantec Endpoint Protection Manager consoles" on page 102.

See "Displaying a message for administrators to see before logging on Symantec Endpoint Protection Manager" on page 101.

See "About administrator account roles and access rights" on page 271.

See "About accepting the self-signed (SSL) server certificate for Symantec Endpoint Protection Manager" on page 99.

See "Increasing the time period for staying logged on to the console" on page 105.

Displaying a message for administrators to see before logging on Symantec Endpoint Protection Manager

You can create and display a customizable message that all administrators see before they can log on to the console. You can display any message. The most common purpose is to display a legal notice to tell the administrators that they are about to log on to a proprietary computer.

The message appears in the console after administrators type their user name and password and click **Log On**. After administrators have read the message, they can acknowledge the notice by clicking **OK**, which logs on the administrators. If administrators click **Cancel**, the logon process is canceled, and the administrator is taken back to the logon window.

The message also appears if the administrator runs the reporting functions from a stand-alone Web browser that is connected to the management server.

To display a message for administrators to see before logging on Symantec Endpoint Protection Manager

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

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

3   Select the domain for which you want to add a logon banner.

4   Under **Tasks**, click **Edit Domain Properties**.

5   On the **Logon Banner** tab, check **Provide a legal notice to administrators when they log on to Symantec Endpoint Protection Manager**.

6   Type the banner title and text. Click **Help** for more information.

7   Click **OK**.

See "About domains" on page 265.

See "Adding a domain" on page 267.

Granting or blocking access to remote Symantec Endpoint Protection Manager consoles

By default, all consoles are granted access. Administrators can log on to the main console locally or remotely from any computer on the network.

You can secure a management console from remote connections by denying access to certain computers.

You may want to grant or deny access from the following types of users or computers:

■   You should deny access to anyone on the Internet. Otherwise, the console is exposed to Internet attacks.

■   You should deny access to limited administrators who use consoles on a different network than the network they manage.

■   You should grant access to system administrators.

■   You should grant access to IT administrators.

■ You should grant access to lab computers, such as a computer that is used for testing.

In addition to globally granting or denying access, you can specify exceptions by IP address. If you grant access to all remote consoles, the management server denies access to the exceptions. Conversely, if you deny access to all remote consoles, you automatically grant access to the exceptions. When you create an exception, the computer that you specified must have a static IP address. You can also create an exception for a group of computers by specifying a subnet mask. For example, you may want to grant access in all areas that you manage. However, you may want to deny access to a console that is located in a public area.

To grant or deny access to a remote console

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

2   Under **Servers**, select the server for which you want to change the remote console access permission.

3   Under **Tasks**, click **Edit the server properties**.

4   On the **General** tab, click **Granted Access** or **Denied Access**.

5   If you want to specify IP addresses of the computers that are exempt from this console access permission, click **Add**.

     Computers that you add become exceptions. If you click **Granted Access**, the computers that you specify are denied access. If you click **Denied Access**, the computers that you specify are granted access. You can create an exception for a single computer or a group of computers.

6   In the **Deny Console Access** dialog box, click one of the following options:

     ■ **Single Computer**
        For one computer, type the IP address.

     ■ **Group of Computers**
        For several computers, type both the IP address and the subnet mask for the group.

7   Click **OK**.

     The computers now appear in the exceptions list. For each IP address and mask, its permission status appears.

     If you change **Granted Access** to **Denied Access** or vice versa, all exceptions change as well. If you have created exceptions to deny access, they now have access.

8 Click **Edit All** to change the IP addresses or host names of those computers that appear on the exceptions list.

The **IP Address Editor** appears. The **IP Address Editor** is a text editor that lets you edit IP addresses and subnet masks.

9 Click **OK**.

10 When you finish adding exceptions to the list or editing the list, click **OK**.

See "Adding an administrator account" on page 273.

See "Logging on to the Symantec Endpoint Protection Manager console" on page 99.

Unlocking an administrator's account after too many logon attempts

For added security, Symantec Endpoint Protection Manager locks out an administrator for a certain length of time after a number of unsuccessful logon attempts. By default, the management server locks out an administrator after five attempts and for 15 minutes.

If you get locked out of your account, you can do one of the following tasks:

- If there is only one system administrator account in the management server, wait for 15 minutes and then log on to Symantec Endpoint Protection Manager. The default system administrator account is admin.

- Log on to Symantec Endpoint Protection Manager using an account with the same or a higher access level, and unlock your account.
  See "About administrator account roles and access rights" on page 271.

To unlock an administrator's account after too many logon attempts

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

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

3 Under **Administrators**, select the administrator account that is locked.

4 Under **Tasks**, click **Edit the administrator**.

5 On the **General** tab, uncheck **Lock the account after the specified number of unsuccessful logon attempts**.

You can also keep the locking feature enabled, but increase the number of unsuccessful logon attempts that are permitted before the account is locked. You can also increase or decrease the amount of time you have to wait until the account unlocks.

6   Click **OK**.

    See "Sending a temporary password to an administrator" on page 284.

    See "Changing the password for an administrator account" on page 283.

Increasing the time period for staying logged on to the console

To help protect the console, the console requires you to reenter your user name and password after one hour. You can increase the timeout period so that you do not have to constantly log on to the management console.

To increase the time period for staying logged on to the console

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

2   Click **Local Site** or a remote site and click **Edit Site Properties**.

3   On the **General** tab, click the **Console Timeout** drop-down list and select **Never**.

4   Click **OK**.

What you can do from the console

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

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

Table 3-1   Symantec Endpoint Protection Manager console pages

Page	Description
Home	Display the security status of your network.
	You can do the following tasks from the Home page:
	■ Obtain a count of detected viruses and other security risks.
	■ Obtain a count of unprotected computers in your network.
	■ Obtain a count of computers that received virus definition and other content updates.
	■ View license status.
	■ Adjust console preferences.
	■ Get information about the latest Internet and security threats.
	See "Configuring reporting preferences" on page 613.
	See "Checking license status" on page 119.
Monitors	Monitor event logs that concern Symantec Endpoint Protection Manager and your managed computers.
	You can do the following tasks from the Monitors page:
	■ View risk distribution graphs.
	■ View event logs.
	■ View the status of recently issued commands.
	■ View and create notifications.
	See "Viewing and acknowledging notifications" on page 640.
Reports	Run reports to get up-to-date information about computer and network activity.
	You can do the following tasks from the Reports page:
	■ Run Quick Reports.
	■ Run the Daily Summary Report.
	■ Run the Weekly Summary Report.
	See "Running and customizing quick reports" on page 618.

Table 3-1   Symantec Endpoint Protection Manager console pages *(continued)*

Page	Description
Policies	Display the security policies that define the protection technology settings.
	You can do the following tasks from the Policies page:
	■ View and adjust the protection settings.
	■ Create, edit, copy, and delete security policies.
	■ Assign security policies to computer groups.
	■ Configure LiveUpdate settings for client computers.
	See "The types of security policies" on page 293.
	See "Performing the tasks that are common to all policies" on page 290.
	See "Managing content updates" on page 546.
Clients	Manage computers and groups.
	You can do the following tasks from this page:
	■ Create and delete groups.
	■ Edit group properties.
	■ View the security policies that are assigned to groups.
	■ Run commands on groups.
	■ Assign the client software to computers in your network.
	See "Managing groups of clients" on page 207.

Table 3-1 Symantec Endpoint Protection Manager console pages *(continued)*

Page	Description
Admin	Manage Symantec Endpoint Protection Manager settings, licenses, and administrator accounts.
	You can do the following tasks from the Admin page:
	■ Increase the time that you are logged on to Symantec Endpoint Protection Manager.
	■ Create, edit, and delete administrator accounts.
	■ View and edit email and proxy server settings.
	■ Import and purchase licenses.
	■ Adjust the LiveUpdate schedule for Symantec Endpoint Protection Manager.
	■ Download content updates from LiveUpdate.
	■ View LiveUpdate status and recent downloads.
	■ Manage Symantec Endpoint Protection Manager domains.
	■ Add, delete, and export client install packages.
	See "Increasing the time period for staying logged on to the console" on page 105.
	See "Managing domains and administrator accounts" on page 269.
	See "Managing content updates" on page 546.

Managing product licenses

This chapter includes the following topics:

- Licensing Symantec Endpoint Protection

- About the trialware license

- About purchasing licenses

- Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license

- About product upgrades and licenses

- About renewing your Symantec Endpoint Protection license

- Checking license status

- About the licensing enforcement rules

- Backing up your license files

- Recovering a deleted license

- Purging obsolete clients from the database to make more licenses available

- About multi-year licenses

- Licensing an unmanaged client

Licensing Symantec Endpoint Protection

Symantec Endpoint Protection requires a paid license after the trial period expires or when your current license expires. You can apply an existing license to a product upgrade.

You use the License Activation Wizard to activate new or renewed licenses, or when you convert a trial license to a paid license. You license Symantec Endpoint Protection according to the number of Symantec Endpoint Protection clients that you need to protect the endpoints at your site.

Once the Symantec Endpoint Protection Manager is installed, you have 60 days to purchase enough license seats to cover all of your deployed clients.

Note: To administer licenses, you must log on to Symantec Endpoint Protection Manager with a management server system administrator account, such as the default account admin.

See "About administrator account roles and access rights" on page 271.

Table 4-1 lists the tasks that are required to purchase, activate, and manage your Symantec product license.

Table 4-1   Licensing tasks

Task	Description
Check the product license requirements	Understand the importance of the license requirements for the computers that you want to protect. A license lets you install the Symantec Endpoint Protection client on a specified number of computers. A license lets you download virus definitions, security content, and product updates from LiveUpdate. See "Product license requirements" on page 82. See "About the licensing enforcement rules" on page 120. See "About multi-year licenses" on page 123.

Table 4-1   Licensing tasks *(continued)*

Task	Description
Purchase a license and save it to the management server	You need to purchase a license in the following situations: ■ You want to purchase Symantec Endpoint Protection. ■ Your trialware license expired. ■ Your paid license expired. ■ Your license is over-deployed. ■ Your upgrade license from Symantec Endpoint Protection 11.x expired. Starting with version 12.1, you do not need to manually download a license file. Depending on the method that you used to purchase your license, a Symantec license file (.slf) or a license serial number is sent to you in an email. See "About purchasing licenses" on page 112. See "Checking license status" on page 119. See "About the trialware license" on page 112.
Import the license file and activate your purchased license	You use the License Activation Wizard in the Symantec Endpoint Protection Manager to import and activate your Symantec product license. Before you activate the license, you must have: ■ A Symantec license serial number ■ A Symantec license file (.slf) You receive one or the other of these when you purchase a license. See "Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license" on page 114. See "About the Symantec Licensing Portal" on page 118.
Back up your license files	Back up your license files to preserve the license files in case the database or the computer's hard disk becomes damaged. See "Backing up your license files" on page 121. See "Recovering a deleted license" on page 121.

Task	Description
Review the preconfigured license notifications	Preconfigured license notifications alert administrators about expired licenses and other license issues. See "What are the types of notifications and when are they sent?" on page 635.
Keep track of when your licenses expire, and renew your licenses	Check the status for each license that you imported into the console to see whether you need to renew a license, or purchase more licenses. See "Checking license status" on page 119. See "About renewing your Symantec Endpoint Protection license" on page 119.

Table 4-1   Licensing tasks *(continued)*

About the trialware license

The trialware license lets you evaluate and test Symantec Endpoint Protection in your environment.

The trialware license applies to the following Symantec Endpoint Protection components:

- Symantec Endpoint Protection Manager

- Symantec Endpoint Protection client

- Access to LiveUpdate content

After the trialware license expires, you must activate a paid license to retain full product functionality. You do not have to uninstall the trial-licensed version to convert your Symantec Endpoint Protection installation to a fully licensed installation.

The trialware license expires 60 days after you install the product.

See "Planning the installation" on page 69.

See "About purchasing licenses" on page 112.

About purchasing licenses

You need to purchase a license in the following situations:

- Your trial license expired. Symantec Endpoint Protection comes with a trialware license that lets you install and evaluate the product in your environment.

- Your current license is expired.

- Your current license is over-deployed. Over-deployed means that you have deployed more instances of the client or Symantec Endpoint Protection Manager than your current license allows for.

- You decide to keep the new version after the upgrade trial from Symantec Endpoint Protection 11.x expires. If you use Symantec Endpoint Protection 11.x, Symantec sends you an email with an upgrade offer that includes a free upgrade trial. If you decide to keep the new version beyond the upgrade trial period of 90 days, you need to purchase a paid license.

Depending upon how you purchase your license, you receive either a product license serial number or a Symantec License file. License files are either sent to you in email or downloaded from a secure Web site. The license file uses the file extension .slf. When you receive the license file by email, it is attached to the email as a .zip file. You must extract the .slf file from the .zip file.

Save the license file to a computer that can be accessed from the Symantec Endpoint Protection Manager console. Many users save the license on the computer that hosts the Symantec Endpoint Protection Manager. Many users also save a copy of the license to a different computer or removable storage media for safekeeping.

Warning: To prevent corruption of the license file, do not open or alter the file contents in any way. You may however, copy and store the license as desired.

Table 4-2 displays where to learn more about purchasing licenses.

Table 4-2 Purchasing license tasks

Task	Description
Determine your licensing requirements	See "Product license requirements" on page 82. See "About the licensing enforcement rules" on page 120.

Table 4-2   Purchasing license tasks *(continued)*

Task	Description
Find out where to buy product licenses	You can purchase a Symantec product license from the following sources: ■ The Symantec online store: http://store.symantec.com/ ■ Your preferred Symantec reseller: To find a reseller, use the Partner locator To find out more about Symantec partners, go to http://www.symantec.com/partners/index.jsp ■ The Symantec sales team: Visit the Symantec Ordering Web site for sales contact information.
Learn more about upgrading from the trialware license that comes with Symantec Endpoint Protection	See "About the trialware license" on page 112.
Get help with purchasing licenses or learn more about licenses	http://customercare.symantec.com/

See "Licensing Symantec Endpoint Protection" on page 109.

Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license

You can use the License Activation Wizard workflow to perform the following tasks:

■ Activating a new paid license.

■ Converting a trial license to a paid license.

■ Renewing a license.

■ Activating a license after you upgrade from a previous version, such as Symantec Endpoint Protection 11.x.

■ Activating an additional paid license in response to an over-deployment status.

You can import and activate a license file that you received from the following sources:

- Symantec Licensing Portal

- Symantec partner or preferred reseller

- Symantec sales team

- Symantec Business Store

Note: You can import your Symantec Network Access Control 12.1 license into a Symantec Network Access Control-enabled management server only.

You can start the License Activation Wizard in the following ways:

- The Symantec Endpoint Protection Welcome screen that appears after you install the product.

- From the **Common Tasks** menu on the **Home** page.

- The **Admin** page of the Symantec Endpoint Protection Manager console.

If you activate or import your license from the Welcome screen or the **Common Tasks** menu, you can skip the first three of the following steps.

To activate or import your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license

1   On the Symantec Endpoint Protection Manager console, click **Admin**.

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

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

4   In the **License Activation Wizard**, select **Activate a new license**, and then click **Next**. If you do not see this panel, continue to the next step.

5 On the **License Activation** panel, select the option that matches your situation, and then click **Next**.

The following table describes each option:

Option	Description
I have a serial number	You may receive a license serial number when you or your Symantec Partner purchased the license. If you have a license serial number, select this option.
	If you are an eFlex (Symantec Enterprise Options) customer and have an eFlex-generated serial number, select **I have a Symantec License File**.
I have a Symantec License File (.slf)	In most cases, a Symantec license file (.slf file) is sent to you in an email from Symantec shortly after you complete the purchase process. The file arrives attached to the notification email as a .zip file. If you have received a .slf file, select this option.
	Note: You must extract the .slf file from the .zip file before you can use it to activate your product license.
	Warning: The .slf file contains the information that is unique to your license. To avoid corrupting the license file, do not alter its contents. You may copy the file for your records.

You can find information about eFlex at the following URL:

Enterprise Options

6 Do one of the following tasks based on the selection that you made in the previous step:

- If you selected **I have a serial number**, enter the serial number, and then click **Submit**. Review the information about the license you added, and then click **Next**.

- If you selected **I have a Symantec License File (.slf)**, click **Add File**. Browse to and select the .slf file you extracted from the .zip file that was attached to your Symantec notification email. Click **Open**, and then click **Next**.

7 Enter information about your technical contacts and primary contacts, and about your company. Click to acknowledge the disclosure statement, and then click **Submit**.

If you provided this information when you purchased your license, this panel does not display.

8 Click **Finish**.

You can also view a video walkthrough of Symantec Endpoint Protection.

To view the video walkthrough

1 Go to http://go.symantec.com/education_septc.

2 On the linked page, click **Symantec Endpoint Protection 12.1**.

3 On the expanded list, click **Symantec Endpoint Protection 12.1: How to Activate the License**.

See "About the trialware license" on page 112.

See "About renewing your Symantec Endpoint Protection license" on page 119.

See "About purchasing licenses" on page 112.

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

See "Licensing Symantec Endpoint Protection" on page 109.

Required licensing contact information

During the activation process, you are asked to provide any missing license contact information. Privacy statements are provided in the wizard to describe how this information is used. You must indicate that the privacy conditions are acceptable before you can complete the activation process.

Table 4-3 includes the information you need.

Table 4-3   Licensing contact information

Type of information	Description
Technical Contact	Contact information for the person who is in charge of the technical activities that are concerned with installing or maintaining your endpoint security infrastructure. The contact's name, email address, and phone number are required.

Table 4-3   Licensing contact information *(continued)*

Type of information	Description
Primary Contact	Contact information for the person who represents your company. The contact's name, email address, and phone number are required. **Note:** Click the checkbox to indicate when the Technical Contact and Primary Contact are the same person.
Company Information	Includes the company name, location, phone number, and email address.

See "Licensing Symantec Endpoint Protection" on page 109.

About the Symantec Licensing Portal

You can use the Symantec Licensing Portal to activate product licenses. However, you can activate licenses from the Symantec Endpoint Protection Manager console, which is simpler and faster.

The Symantec Licensing Portal is at the following location:

https://licensing.symantec.com

Additional information about using the Symantec Licensing Portal to manage licenses is available at the Symantec Customer Care Web site:

http://customersupport.symantec.com/

Note: You must create an account before you can use the licensing portal. If you do not have a Symantec Licensing Portal account, a link is provided on the main page to create one.

See "Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license" on page 114.

See "Licensing Symantec Endpoint Protection" on page 109.

About product upgrades and licenses

When Symantec releases a new version of Symantec Endpoint Protection, you may apply your existing active license to the new version. You receive an email notification that a new release is available that includes instructions for downloading the new version of Symantec Endpoint Protection.

For more information about licensing product upgrades, see the Version Upgrade FAQ at the following URL:

http://www.symantec.com/business/products/upgrades/faq/index.jsp

See "Upgrading to a new release of Symantec Endpoint Protection" on page 156.

About renewing your Symantec Endpoint Protection license

When your current license is about to expire, the Symantec Endpoint Protection Manager sends license expiration notifications to the Symantec Endpoint Protection administrator. Symantec highly recommends that you renew your license before it expires.

When you renew a license, the management server removes and replaces the expired license with a new license. To purchase renewal licenses, visit the Symantec Store, or contact your Symantec partner or preferred Symantec reseller.

In the event that you accidentally delete a license, you can recover it from the Symantec Endpoint Protection Manager console.

See "About purchasing licenses" on page 112.

See "Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license" on page 114.

See "Recovering a deleted license" on page 121.

Checking license status

You can find out whether the management server uses a trialware license or a paid license. You can also obtain the following license information for each paid license that you imported into the console:

- **License serial number, total seat count, expiration date**

- **Number of valid seats**

- **Number of deployed seats**

- **Number of expired seats**

- **Number of over-deployed clients**

The license status is not available for a trialware license.

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

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

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

To check license status for paid licenses

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

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

See "Licensing Symantec Endpoint Protection" on page 109.

See "Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license" on page 114.

About the licensing enforcement rules

Symantec Endpoint Protection licenses are enforced according to the following rules:

Table 4-4   Licensing enforcement rules

Where applies	Rule
Term of license	The term of the license starts from the time and date of activation until midnight of the last day of the licensing term.
	If you have multiple sites, the license expires on the day and the time of the westernmost Symantec Endpoint Protection Manager database.
License coverage: Symantec Endpoint Protection components	A Symantec Endpoint Protection license applies to the Symantec Endpoint Protection clients. For instance, in a network with 50 endpoints, the license must provide for a minimum of 50 seats. Instances of the Symantec Endpoint Protection Manager do not require a license.
License coverage: sites and domains	A Symantec Endpoint Protection product license is applied to an entire installation regardless of the number of replicated sites or domains that compose the installation. For instance, a license for 100 seats covers a two-site installation where each site has 50 seats.
	If you have not implemented replication, you may deploy the same .slf file to multiple Symantec Endpoint Protection management servers. The number of clients reporting to your management servers must not exceed the total number of licensed seats.

Where applies	Rule
License coverage: platforms	Licensing seats apply to clients running on any platform, whether the platform is Windows or Mac.
License coverage: products and versions	License seats apply equally across product versions. For example, a license covers both version 11.x and 12.1.x clients within the same site.

Table 4-4 Licensing enforcement rules *(continued)*

See "Licensing Symantec Endpoint Protection" on page 109.

Backing up your license files

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

By default, when you import the license file using the Licensing Activation Wizard, Symantec Endpoint Protection Manager places a copy of the license file in the following location: *Symantec Endpoint Protection Manager installation directory*\Inetpub\license

If you misplaced the license files you originally downloaded or received by email, you can download the files again from the Symantec Licensing Portal Web site.

To back up your license files

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

See your company's procedure for backing up files.

See "Activating or importing your Symantec Endpoint Protection or Symantec Network Access Control 12.1 product license" on page 114.

See "About the Symantec Licensing Portal" on page 118.

See "Licensing Symantec Endpoint Protection" on page 109.

Recovering a deleted license

If you accidentally delete a license file, you can recover it from the Symantec Endpoint Protection Manager console.

To recover a deleted license

1   On the Symantec Endpoint Protection Manager console **Admin** page, click **Licenses** and then under **Tasks**, click **Recover a deleted license**.

2   On **License recovery** panel, check the deleted license you want to recover, and then click **Submit**.

Purging obsolete clients from the database to make more licenses available

Symantec Endpoint Protection Manager can incorrectly display an over-deployed license status due to obsolete clients. These are database entries for the clients that no longer communicate with Symantec Endpoint Protection Manager in the protected environment. Clients can be rendered obsolete for many reasons, such as when you upgrade the operating system, decommission a computer, or change the hardware configuration.

Obsolete clients count against the product license, so it is important to purge obsolete clients as soon as they are created. If your license reports show more seats are licensed than known to be deployed, you should purge the database of obsolete clients. By default, purging occurs every 30 days. Shorten the interval between purge cycles to more quickly purge the obsolete clients. You reset the interval as needed to suit your long-term needs after the purge cycle completes.

In non-persistent Virtual Desktop Infrastructures (VDIs), you can set a separate time period for purging the non-persistent clients. This setting purges the offline clients that have not connected during the time period that you set. Non-persistent offline clients do not affect the license count.

To purge obsolete clients from the database

1   In the Symantec Endpoint Protection Manager, on the **Admin** page, click **Domains**.

2   In the **Domains** tree, select the desired domain.

3   Under **Tasks**, click **Edit Domain Properties**.

4   On the **Edit Domain Properties > General** tab, change the specified time to delete the clients that have not connected from the default of **30** days to *1*.

    You do not need to set the option to purge the non-persistent clients for licensing purposes. The non-persistent clients that are offline do not count toward the license total.

5 Click **OK**.

6 Wait 24 hours and then revert the settings to 30 days or to another interval that suit your requirements.

See "Licensing Symantec Endpoint Protection" on page 109.

About multi-year licenses

When you purchase a multi-year license, you receive a set of license files equal to the number of years your license is valid. For instance, a three-year license consists of three separate license files. When you activate a multi-year license, you import all of the license files during the same activation session. The Symantec Endpoint Protection Manager merges the separate license files into a single activated license that is valid for the purchased duration.

While not recommended, it is possible to activate fewer than the full complement of license files. In this case, the Symantec Endpoint Protection Manager merges the files and applies the duration of the license file that expires last. For instance, a three-year license that is activated with only the first two files indicates a duration of only two years. When the third file is activated at a later date, the full duration of the license is reported accurately as three years. In all cases, the number of seats remains consistent with the number of seats that you purchased.

When the Symantec Endpoint Protection Manager merges files, the shortest duration files are deleted and the longest duration file is kept for internal license-keeping functions. If you think that a license was deleted inappropriately, recover and reactivate the deleted license.

You can see the license serial numbers of shorter duration that are associated with the active license. On the **Admin** page, click **Licenses** and then click the activated license. The associated licenses appear in the **Associated Licenses** column.

See "Recovering a deleted license" on page 121.

See "Licensing Symantec Endpoint Protection" on page 109.

Licensing an unmanaged client

To enable the submission of reputation data from an unmanaged client, you must install a paid license on the unmanaged client.

To license an unmanaged client

1   Locate and create a copy of your current Symantec Licensing File (.slf).

      Use the same file that you used to activate your license on Symantec Endpoint Protection Manager.

2   On the client computer, place the copied license file into the Symantec Endpoint Protection client inbox.

      ■   On the clients that run on a pre-Vista version of Windows, the inbox is located at: *Drive*:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox

      ■   On the clients that use Vista or a later version of Windows, the inbox is located at: *Drive*:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox\

      If the license file is invalid or the license installation failed, a folder named `Invalid` is created and the invalid license is placed into the folder. If the file is valid, it is automatically removed from the inbox after it is processed.

3   To verify that you applied the license correctly, check that no files appear in the inbox folder.

4   Check that the .slf file is in either one of the following folders:

      ■   For the clients that run on a pre-Vista version of Windows: *Drive*:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection*silo_identification*\Data\Config

      ■   For the clients that run on Vista or a later version of Windows: *Drive*:\ProgramData\Symantec\Symantec Endpoint Protection*silo_identification*\Data\Config

You can also include the .slf file as part of a third-party deployment package.

Installing the Symantec Endpoint Protection client

This chapter includes the following topics:

- Preparing for client installation
- About client deployment methods
- Exporting client installation packages
- About the client installation settings
- Configuring client installation package features
- Configuring client packages to uninstall existing third-party security software
- Restarting client computers
- About managed and unmanaged clients
- Installing an unmanaged client
- Uninstalling the Windows client
- Uninstalling the Mac client
- Managing client installation packages
- Adding client installation package updates

Preparing for client installation

Table 5-1 lists the actions that you must perform before you can install the client software on the computers in your network.

Table 5-1   Client computer preparation

Action	Description
Identify client computers	Identify the computers on which you want to install the client software. All the computers must run a supported operating system.
	For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control
	Note: Symantec recommends that you also install the client on the computer that hosts Symantec Endpoint Protection Manager.
Identify computer groups	Identify the computer groups to which you want the clients to belong. You can group clients based on type of computer, to conform to your corporate organization, or the security level required. You can create these groups if you have not already done so. You can also import an existing group structure such as an Active Directory structure.
	See "Managing groups of clients" on page 207.
	See "Importing existing groups and computers from an Active Directory or an LDAP server" on page 211.
	See "Assigning clients to groups before you install the client software" on page 217.
Prepare computers for remote deployment	Prepare the computers for remote client deployment.
	■ Modify firewall settings to allow communication between Symantec Endpoint Protection components. See "About firewalls and communication ports" on page 129. See "Preparing Windows operating systems for remote deployment" on page 127. ■ Uninstall any legacy Symantec virus protection software if the migration is not supported. See "Supported and unsupported migration paths to Symantec Endpoint Protection" on page 179. See the Symantec documentation for your legacy Symantec virus protection software for information about uninstallation.
	Note: If your users do not have administrative rights for their computers, then remotely install the client software using Remote Push. The Remote Push installation requires you to enter the credentials that have local administrative rights for the computers.
	See "Deploying clients by using Remote Push" on page 135.

Table 5-1	Client computer preparation *(continued)*
Action	**Description**
Deploy client software	You deploy the client software using any of the three available methods. You can also export a customized client package before you deploy it.
	See "About client deployment methods" on page 131.
	See "Exporting client installation packages" on page 139.
	■ You decide which features to install to the client computers. See "About the client installation settings" on page 141. See "Configuring client installation package features" on page 142.
	■ You can choose to automatically uninstall existing third-party security software when you create or deploy a client installation package. Otherwise, you must uninstall third-party security software before deployment.
	Note: Some programs may have special uninstallation routines. See the documentation for the third-party software.
	See "Configuring client packages to uninstall existing third-party security software" on page 143.
Verify installation status	You should confirm the status of the clients in the console. Managed clients may not appear in the console until after they are restarted.
	See "Restarting client computers" on page 145.
	You can take additional steps to secure unmanaged computers and optimize the performance of your Symantec Endpoint Protection installation.
	See "About managed and unmanaged clients" on page 146.
	See "Installing an unmanaged client" on page 147.
	See "Getting up and running on Symantec Endpoint Protection for the first time" on page 51.

Preparing Windows operating systems for remote deployment

Table 5-2 lists the associated tasks that you must do on client computer operating systems to successfully install the client remotely.

| Table 5-2 | Remote deployment actions |

Operating system	Tasks
Prepare Windows XP computers or Windows Server 2003 servers that are installed in workgroups	Windows XP computers and Windows Server 2003 servers that are installed in workgroups do not accept remote deployment by default. To permit remote deployment, disable Simple File Sharing. **Note:** This limitation does not apply to computers that are part of a Windows domain. You may also need to perform the following tasks: ■ Ensure that the Administrator account does not have a blank password. ■ Disable the Windows Firewall, or allow the ports that are required for communication between Symantec Endpoint Protection and Symantec Endpoint Protection Manager. See "About firewalls and communication ports" on page 129.
Prepare Windows Vista, Windows 7, or Windows Server 2008 computers	Windows User Account Control blocks local administrative accounts from remotely accessing remote administrative shares such as C$ and Admin$. You do not need to fully disable User Account Control on the client computers during the remote deployment if you disable the registry key LocalAccountTokenFilterPolicy. For more information, visit the following URL: http://support.microsoft.com/kb/951016 To push the client software to computers, you should use a domain administrator account if the client computer is part of an Active Directory domain. Remote deployment also requires administrator privileges to install. Perform the following tasks: ■ Disable the Sharing Wizard. ■ Enable network discovery by using the Network and Sharing Center. ■ Enable the built-in administrator account and assign a password to the account. ■ Verify that the account has administrator privileges.
Prepare Windows 8 or Windows Server 2012 computers	Before you deploy, perform the following tasks: ■ Disable the Windows Firewall. ■ Create the registry key LocalAccountTokenFilterPolicy. For more information, visit the following URL: http://support.microsoft.com/kb/942817 ■ Enable and start the Remote Registry service.

See your Windows documentation for more information.

See "Preparing for client installation" on page 125.

About firewalls and communication ports

If your Symantec Endpoint Protection Manager and client computers run firewall software, you must open certain ports for communication between the management server and clients. See your firewall software product documentation for instructions to open ports or allow applications to use ports.

Warning: The firewall in the Symantec Endpoint Protection client is disabled by default at initial installation. To ensure firewall protection, leave the Windows firewall enabled on the clients until the software is installed and the client is restarted. The Symantec Endpoint Protection client firewall automatically disables the Windows firewall when the computer restarts.

Table 5-3   Ports for client and server installation and communication

Function	Component	Protocol and port
Push deployment	Management server and client	TCP 139 and 445 on management servers and clients UDP 137 and 138 on management servers and clients TCP ephemeral ports on management servers and clients
Group Update Provider communication	Management server and Group Update Provider Group Update Provider and clients	TCP 2967 on all devices **Note:** You can change this default port.
General communication	Management server and client	For management servers and clients: ■ TCP 8014 for management servers, by default. You can change TCP 8014 (HTTP) to TCP 443 (HTTPS). ■ TCP ephemeral port on clients. For remote management servers and consoles: ■ TCP 8443 for remote management servers and console ■ TCP ephemeral ports and 9090 on consoles ■ TCP 8445 for remote reporting consoles
Replication communication	Site to site between database servers	TCP 8443 between database servers

Table 5-3   Ports for client and server installation and communication
                     (continued)

Function	Component	Protocol and port
Remote Symantec Endpoint Protection Manager console installation	Management server and remote management server console	TCP 9090 on remote management servers TCP ephemeral ports on remote consoles **Note:** You can change the port.
Web services	Remote Monitoring and Management (RMM) Symantec Protection Center 2.x	TCP 8446 for RMM Web services TCP 8444 for Symantec Protection Center 2.x Web services
External database communication	Remote Microsoft SQL Servers and management server	TCP 1433 on remote Microsoft SQL Servers TCP ephemeral ports on management servers **Note:** Port 1433 is the default port.
Symantec Network Access Control Enforcer communication	Management server and Enforcer	TCP 1812 on management servers TCP ephemeral ports on enforcers **Note:** RADIUS servers also use port 1812; do not install the management server on the same server. You cannot change the port on the management server. Client authentication by the Enforcer on UDP 39,999
Migration and client deployment	Symantec Endpoint Protection Manager and legacy Symantec management server	TCP 139, TCP 445, TCP ephemeral ports, and UDP 137
LiveUpdate	LiveUpdate client and server	TCP ephemeral ports on clients TCP 80 on LiveUpdate servers

- Windows Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012 contain a firewall that is enabled by default. If the firewall is enabled, you might not be able to install or deploy the client software remotely. If you have problems deploying the client to computers running these operating systems, configure their firewalls to allow the required traffic.

- If you have legacy Symantec virus protection software in your environment, open TCP and UDP port 2967, if they are not already open.

- If you decide to use the Windows firewall after deployment, you must configure it to allow file and printer sharing (port 445).

For more information about configuring Windows firewall settings, see the Windows documentation.

See "Enabling and disabling a firewall policy" on page 420.

See "Monitoring endpoint protection" on page 603.

See "Preparing for client installation" on page 125.

About client deployment methods

You deploy the Symantec Endpoint Protection client by using the Client Deployment Wizard. You deploy the client software after the Symantec Endpoint Protection Manager is installed.

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

Table 5-4 displays the client deployment methods that you can use.

Table 5-4 Client deployment options

Options	Description
Web link and email	Users receive an email message that contains a link to download and install the client software. The users must have local administrator rights to their computers. Web link and email notification installation is the recommended deployment method. See "Deploying clients using a Web link and email" on page 132.
Remote push	Remote push installation lets you control the client installation. Remote push installation pushes the client software to the computers that you specify. The installation begins automatically. See "Preparing Windows operating systems for remote deployment" on page 127. See "Deploying clients by using Remote Push" on page 135.
Save package	Custom installation creates an executable installation package that you save to the management server and then distribute to the client computers. Users run a setup.exe file to install the client software. See "Deploying clients by using Save Package" on page 137.

See "Which features should you install on the client?" on page 132.

See "Preparing for client installation" on page 125.

Which features should you install on the client?

When you deploy the client using the Client Deployment Wizard, you must choose the feature set. The feature set includes multiple protection components that are installed on the client. You can select a default feature set or select individual components. Decide which feature set to install based on the role of the computers, and the level of security or performance that the computers need.

Table 5-5 lists the protection technologies you should install on client computers based on their role.

Table 5-5   Recommended feature set by computer role

Client computer role	Recommended feature set
Workstations, desktop, and laptop computers	**Full Protection for Clients** Includes all protection technologies. Appropriate for laptops, workstations, and desktops. Includes the full download protection and mail protocol protection. **Note:** Whenever possible, use Full Protection for maximum security.
Servers	**Full Protection for Servers** Includes all protection technologies except mail protocol protection. Appropriate for any servers that require maximum network security.
High-throughput servers	**Basic Protection for Servers** Includes Virus and Spyware Protection and Download Protection. Appropriate for any servers that require maximum network performance.

See "Configuring client installation package features" on page 142.

See "About client deployment methods" on page 131.

See "Preparing for client installation" on page 125.

Deploying clients using a Web link and email

The Web link and email method creates a URL for each client installation package. You send the link to users in an email or make it available from a network location.

Web link and email performs the following actions:

- Selects and configures the client installation packages.
  Client installation packages are created for 32-bit and 64-bit Windows computers. The installation packages are stored on the computer that runs Symantec Endpoint Protection Manager.

- Notifies the computer users about the client installation packages.
  An email message is sent to the selected computer users. The email message contains instructions to download and install the client installation packages. Users follow the instructions to install the client software.

The Mac client install package is automatically exported as a `.zip` archive file. To expand the package and extract the folder containing the Apple installer file (`.pkg`) and the `Additional Resources` folder, you must use either the Mac `Archive Utility` or the `ditto` command. You cannot use the Mac `unzip` command, a third-party application, or any Windows application to expand this file. You must keep the `.pkg` file and the `Additional Resources` folder together to complete the installation successfully.

Before you deploy the client installation package with email, make sure that you correctly configure the connection from the management server to the mail server.

You start the client deployment from the console.

To deploy clients by using a Web link and email

1   In the console, on the **Home** page, in the **Common Tasks** menu, select **Install protection client to computers**.

2   In the **Client Deployment Wizard**, click **New Package Deployment** to create a new installation package, and then click **Next**.

   Existing Package Deployment lets you deploy the packages that have been exported previously, but you can only use Remote Push with this option.

   Communication Update Package Deployment lets you update client communication settings on the computers that already have the client installed. Use this option to convert an unmanaged client to a managed client. You can only use Remote Push or Save Package with this option.

   See "Deploying clients by using Remote Push" on page 135.

   See "Deploying clients by using Save Package" on page 137.

   See "Restoring client-server communications by using a client installation package" on page 701.

3 For a new package, make selections from **Install Packages**, **Group**, **Install Feature Sets**, **Install Settings**, **Content Options**, and **Preferred Mode**. Click **Next**.

Note: To uninstall third-party security software on the client, you must configure custom Client Install Settings before launching the Client Deployment Wizard. To see which third-party software the client package removes, see the following knowledge base article: About the third-party security software removal feature in Symantec Endpoint Protection 12.1.

See "Configuring client packages to uninstall existing third-party security software" on page 143.

See "About the client installation settings" on page 141.

4 Click **Web Link and Email**, and then click **Next**.

5 In the **Email Recipients and Message** panel, specify the email recipients and the subject.

To specify multiple email recipients, type a comma after each email address. A management console System Administrator automatically receives a copy of the message.

You can accept the default email subject and body, or edit the text. You can also copy the URL and post it to a convenient online location, like an intranet page.

To create the package and deliver the link by email, click **Next**, and then click **Finish**.

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

Client computers may not appear within the management console until after they are restarted. Depending on the client restart settings of the deployed client, you or the computer users may need to restart the client computers.

See "Restarting client computers" on page 145.

See "Viewing the status of deployed client computers" on page 611.

See "Which features should you install on the client?" on page 132.

See "About client deployment methods" on page 131.

See "Preparing for client installation" on page 125.

See "Establishing communication between the management server and email servers" on page 640.

Deploying clients by using Remote Push

Remote Push lets you control the client installation. Remote Push pushes the client software to the computers that you specify. Using Remote Push requires knowledge of how to search networks to locate computers by IP address or computer names. Once the package is pushed, the installation is performed automatically and does not rely on the computer user to start it.

Remote Push performs the following actions:

■ Selects an existing client installation package or creates a new installation package.

■ For new installation packages, configures package deployment settings.

■ Locates the computers on your network.
Remote Push locates either specific computers for which you provide an IP number or range, or all computers that are visible by browsing the network.

■ Pushes the client software to the computers that you specify.
The installation automatically begins on the computers once the package is successfully pushed.

The Mac client cannot be deployed using Remote Push.

You start the client deployment from the console.

To deploy clients by using Remote Push

1   In the console, on the **Home** page, in the **Common Tasks** menu, click **Install protection client to computers**.

2   In the **Client Deployment Wizard**, do one of the following tasks:

■ Click **New Package Deployment** to create a new installation package, and then click **Next**.

■ Click **Existing Package Deployment** to use a package that was previously created, and then click **Browse** to locate the package to deploy.
The Client Deployment Wizard uploads the package and directs you to the **Computer Selection** panel (step 5).

■ Click **Communication Update Package Deployment** if you want to update client communication settings on the computers that already have the client installed.
Use this option to convert an unmanaged client to a managed client.

See "Restoring client-server communications by using a client installation package" on page 701.

3 For a new package, in the **Select Group and Install Feature Sets** panel, make selections from **Install Packages**, **Group**, **Install Feature Sets**, **Install Settings**, **Content Options**, and **Preferred Mode**. Click **Next**.

To uninstall third-party security software on the client, you must configure custom Client Install Settings before you launch the Client Deployment Wizard. You can also use an existing client install package that is configured to enable this function. To see which third-party software the client package removes, see the following knowledge base article: About the Security Software Removal feature in Symantec Endpoint Protection 12.1.

See "Configuring client packages to uninstall existing third-party security software" on page 143.

See "About the client installation settings" on page 141.

4 Click **Remote Push**, and then click **Next**.

5 In the **Computer Selection** panel, locate the computers to receive the software using one of the following methods:

■ To browse the network for computers, click **Browse Network**.

■ To find computers by IP address or computer name, click **Search Network**, and then click **Find Computers**.

You can set a timeout value to constrain the amount of time that the server applies to a search.

6 Click **> >** to add the computers to the list, and authenticate with the domain or workgroup if the wizard prompts you.

The remote push installation requires elevated privileges.

If the client computer is part of an Active Directory domain, you should use a domain administrator account.

7 Click **Next**, and then click **Send** to push the client software to the selected computers.

Once the **Deployment Summary** panel indicates a successful deployment, the installation starts automatically on the client computers.

The installation takes several minutes to complete.

8   Click **Next**, and then click **Finish**.

9   Confirm the status of the deployed clients on the **Clients** page.

Client computers may not appear within the management console until after they are restarted. Depending on the client restart settings of the deployed client, you or the computer users may need to restart the client computers.

See "Restarting client computers" on page 145.

See "Viewing the status of deployed client computers" on page 611.

See "Preparing Windows operating systems for remote deployment" on page 127.

See "Which features should you install on the client?" on page 132.

See "About client deployment methods" on page 131.

See "Managing domains and administrator accounts" on page 269.

See "Preparing for client installation" on page 125.

Deploying clients by using Save Package

Save Package creates the installation packages that you can install either manually, with third-party deployment software, or with a login script.

Save Package performs the following actions:

■   Creates a 32-bit or 64-bit installation package.
    The installation package can comprise one setup.exe file or a collection of files that includes a setup.exe file. Computer users often find one setup.exe file easier to use.

■   Saves the installation package to a directory on the computer that runs Symantec Endpoint Protection Manager.

You must provide the installation package to the computer users. The users run the setup.exe file to install the client software. You or the computer users must restart the computers after installation. Alternately, you can use third-party deployment software to perform the installation.

The Mac client install package is automatically exported as a `.zip` archive file. To expand the package and extract the folder containing the Apple installer file (`.pkg`) and the `Additional Resources` folder, you must use either the Mac `Archive Utility` or the `ditto` command. You cannot use the Mac `unzip` command, a third-party application, or any Windows application to expand this file. You must keep the `.pkg` file and the `Additional Resources` folder together to complete the installation successfully.

You start the client deployment from the console.

To deploy clients by using Save Package

1   In the console, on the **Home** page, in the **Common Tasks** menu, click **Install protection client to computers**.

2   In the **Client Deployment Wizard**, click **New Package Deployment** to configure a new installation package, and then click **Next**.

    Existing Package Deployment lets you deploy the packages that have been exported previously, but you can only use Remote Push with this option.

    Communication Update Package Deployment lets you update client communication settings on the computers that already have the client installed. Use this option to convert an unmanaged client to a managed client. Click **Next** to select the group of clients on which the package is installed.

    See "Restoring client-server communications by using a client installation package" on page 701.

3   For a new package, make selections from **Install Packages**, **Group**, **Install Feature Sets**, **Install Settings**, **Content Options**, and **Preferred Mode**. Click **Next**.

    Note: To uninstall third-party security software on the client, you must configure custom Client Install Settings before launching the Client Deployment Wizard. To see which third-party software the client package removes, see the following knowledge base article: About the Security Software Removal feature in Symantec Endpoint Protection 12.1.

    See "Configuring client packages to uninstall existing third-party security software" on page 143.

    See "About the client installation settings" on page 141.

4   Click **Save Package**, and then click **Next**.

5   Click **Browse** and specify the folder to receive the package.

    Check **Single .exe file (default)** or **Separate files (required for .MSI)**, and then click **Next**.

    Note: Use **Single .exe file** unless you require separate files for a third-party deployment program.

6   Review the settings summary, click **Next**, and then click **Finish**.

7 Provide the custom installation package to the computer users.

For example, you can save the installation package to a shared network location, or email the installation package to the computer users. You can also use a third-party program to deploy the package.

8 Confirm that the computer users have received and installed the client software, and confirm the status of the deployed clients.

Client computers may not appear within the management console until after they are restarted. Depending on the client restart settings of the deployed client, you or the computer users may need to restart the client computers.

See "Restarting client computers" on page 145.

See "Viewing the status of deployed client computers" on page 611.

See "Which features should you install on the client?" on page 132.

See "About client deployment methods" on page 131.

See "Deploying clients by using Remote Push" on page 135.

See "Preparing for client installation" on page 125.

Exporting client installation packages

You might want to export a client install package if you want to use a third-party distribution system, or an unmanaged client with custom policies.

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

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

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

You must decide whether to create an installation package for managed clients or unmanaged clients. Both types of packages have the features, policies, and settings that you assign. 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. You can convert an unmanaged client to a managed client at any time with **Communication Update Package Deployment** through the **Client Deployment Wizard**.

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 packages, you deploy the installation package on the client computers.

Note: On those computers that run the 64-bit versions of Microsoft Windows operating systems, you deploy the client installation packages with the silent or the unattended option. These 64-bit operating systems include Windows Vista, Windows 7, Windows 8, Windows Server 2008 (including R2), and Windows Server 2012. Only use the silent option for the packages that you deploy to computers running the 32-bit versions of Windows Vista, Windows 7, Windows 8, and Windows Server 2008. When you use a silent deployment, you must restart the applications that plug into Symantec Endpoint Protection, such as Microsoft Outlook and Lotus Notes.

To export client installation packages

1   In the console, click **Admin**, and then click **Install Packages**.

2   Under **Install Packages**, click **Client Install Package**.

3   In the **Client Install Package** pane, under **Package Name**, right-click the package to export and then click **Export**.

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

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

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

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

6   Click **OK**.

See "Managing client installation packages" on page 150.

See "Deploying clients using a Web link and email" on page 132.

See "Restoring client-server communications by using a client installation package"
on page 701.

See "Preparing for client installation" on page 125.

About the client installation settings

The Client Deployment Wizard prompts you to specify the group name and the
protection technologies that you want to install on the client computer.

The protection technologies are grouped in feature sets. You can specify which
feature sets are active on the client computer. You can assign feature sets according
to the client group.

Table 5-6 defines the components within the feature sets that you can install on
the client computer.

Table 5-6   Feature sets

Feature set	Description
Virus, Spyware, and Basic Download Protection	■ **Virus and Spyware Protection** Installs the core virus, spyware, and Download Protection features. Includes Auto-Protect real-time file scanning and manual file scanning. ■ **Advanced Download Protection** Allows you full control over detection aggressiveness. Download Insight detects a malicious file or potentially malicious file when a user tries to download it from a browser or a text messaging client. Download Insight uses reputation information to inspect downloaded files for security problems. ■ **Email Protection** Scans the emails for malicious code as they are sent or received. See "How Symantec Endpoint Protection uses reputation data to make decisions about files" on page 355.

Table 5-6	Feature sets *(continued)*
Feature set	**Description**
Proactive Threat Protection	■ **SONAR** Replaces the TruScan technology in previous versions. SONAR operates in real time to identify malicious behavior of unknown threats. ■ **Application and Device Control** Monitors the applications on client computers and the hardware that connects to client computers. See "About SONAR" on page 395. See "About application and device control" on page 479.
Network Threat Protection	■ **Firewall** Guards against network threats by detecting and blocking inbound and outbound malicious traffic. ■ **Intrusion Prevention** Uses the signatures to identify attacks on client computers. For known attacks, Intrusion Prevention automatically discards the packets that match known threats. See "How a firewall works" on page 415. See "How intrusion prevention works" on page 464.

After installation, you can enable or disable the protection technologies in the security policies.

See "About the types of threat protection that Symantec Endpoint Protection provides" on page 46.

See "Configuring client installation package features" on page 142.

See "About enabling and disabling protection when you need to troubleshoot problems" on page 229.

See "Performing the tasks that are common to all policies" on page 290.

See "Preparing for client installation" on page 125.

Configuring client installation package features

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

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.

For client installation packages for mail servers, under **Virus, Spyware, and Basic Download Protection**, do not check the email scanner protection options. For client installation packages for workstations, check the email scanner protection option that applies to the mail server in your environment. For example, if you use a Microsoft Exchange mail server, check **Microsoft Outlook Scanner**.

Note: Symantec tested and certified the Virus and Spyware Protection components to use in the Federal Desktop Core Configuration (FDCC)-compliant environments.

To configure client installation package features

1   In the console, click **Admin**, and then click **Install Packages**.

2   Under **Install Packages**, click **Client Install Feature Set**.

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.

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

6   Click **OK**.

See "About the client installation settings" on page 141.

See "Managing client installation packages" on page 150.

See "Preparing for client installation" on page 125.

Configuring client packages to uninstall existing third-party security software

You can configure and deploy new installation packages to uninstall existing third-party security software before the installation of the Symantec Endpoint Protection client. Uninstalling third-party security software allows the Symantec Endpoint Protection client to run more efficiently.

You enable the security software removal feature by creating or modifying a custom Client Install Settings configuration. You then select this custom configuration during deployment.

To see which third-party software the client package removes, see the following knowledge base article: About the third-party security software removal feature in Symantec Endpoint Protection 12.1. Some programs may have special uninstallation routines. See the documentation for the third-party software.

Note: You cannot remove third-party security software with Mac or Symantec Network Access Control client packages. You also cannot configure installation packages earlier than Symantec Endpoint Protection client version 12.1.1101 and legacy client versions 11.x to remove third-party security software.

Only the packages you create using the following procedure can remove third-party security software.

To configure client packages to uninstall existing third-party security software

1   In the console, on the **Admin** page, click **Install Packages**, and then click **Client Install Settings**.

2   Under **Tasks**, click **Add Client Install Settings**.

Note: If you have previously created a custom Client Install Settings configuration, you can modify it under **Tasks**, and then click **Edit Client Install Settings...**. Modifying an existing custom configuration does not modify previously exported install packages.

---

3   On the **Basic Settings** tab, check **Automatically uninstall existing security software**, and then click **OK**.

    You can modify other options for this configuration. Click **Help** for more information about these options. Click **OK** again to save the configuration.

4   On the **Home** page, in the **Common Tasks** drop-down list, click **Install protection client to computers**.

5   In the **Client Deployment Wizard**, click **New Package Deployment**, and then click **Next**.

    You can use **Existing Package Deployment** to deploy install packages previously created by **Web link and email** or **Save Package**, or exported through the **Admin** page. However, you must have exported these packages using a custom Client Install Settings configuration like the one described in steps 1 through 3.

6   In **Select Group and Install Feature Set**, in the **Install Settings** drop-down list, click the custom Client Install Settings configuration that you created or modified in step 2. Click **Next**.

7   Choose the deployment method that you want to use: **Web link and email**,
    Remote Push, or **Save Package**.

8   Click **Next** to proceed with and complete your chosen deployment method.

See "Deploying clients using a Web link and email" on page 132.

See "Deploying clients by using Remote Push" on page 135.

See "Deploying clients by using Save Package" on page 137.

See "Preparing for client installation" on page 125.

Restarting client computers

You need to restart client computers after you install the client software. By
default, the client computers restart automatically after installation.

You can configure the restart options on a group to control how the client
computers restart after AutoUpgrade. You can also restart the client computers
at any time by running a restart command from the management server. You
have the option to schedule the client computers to restart during a time that is
convenient for users. You can force an immediate restart, or give the users an
option to delay.

To configure restart options on client computers

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

2   On the **Clients** page, select a group, and then click **Policies**.

3   On the **Policies** tab, click **General Settings**.

4   In the **General Settings** dialog box, on the **Restart Settings** tab, select the
    restart method and schedule.

    Some restart options apply only to Windows clients. For details, see the
    context-sensitive help.

    You can also add a notification that appears on the client computer before
    the restart occurs.

5   Click **OK**.

To restart a selected client computer

1   In the console, click **Clients**

2   On the **Clients** page, on the **Clients** tab, select a group.

3 On the **Clients** tab, select a client, right-click **Run Command on Computers**, and then click **Restart Client Computers**.

4 Click **Yes**, specify the restart options that you require, and then click **OK**.

Some restart options apply only to Windows clients. For details, see the context-sensitive help.

To restart the client computers in a selected group

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

2 On the **Clients** page, on the **Clients** tab, select a group, click **Run a command on the group**, and then click **Restart Client Computers**.

3 Click **Yes**, specify the restart options that you require, and then click **OK**.

Some restart options apply only to Windows clients. For details, see the context-sensitive help.

See "About commands that you can run on client computers" on page 231.

See "Running commands on the client computer from the console" on page 233.

See "Preparing for client installation" on page 125.

About managed and unmanaged clients

You can install the client software as a managed client or as an unmanaged client. In most cases, you should install a managed client. You may want to install an unmanaged client if you want the user to have more control over the computer, such as a test computer. Make sure that the unmanaged client users have the appropriate level of knowledge to configure any security settings that are different from the default settings.

Table 5-7   Differences between a managed and an unmanaged client

Type	Description
Managed client	You administer the clients from the console. Managed client computers connect to your network. You use the console to update the client software, security policies, and virus definitions on the managed client computers.
	In most cases, you install the client software as a managed client.
	You can install a managed client in either of the following ways:
	■ During initial product installation ■ From the console after installation
Unmanaged client	The primary computer user must administer the client computer. An unmanaged client cannot be administered from the console. The primary computer user must update the client software, security policies, and virus definitions on the unmanaged client computer.
	You install an unmanaged client directly from the product disc. You can also export an unmanaged client from the management console, with a group's policies or with the default policies.
	See "Exporting client installation packages" on page 139.
	See "Installing an unmanaged client" on page 147.

See "Why do I need to replace the client-server communications file on the client computer?" on page 698.

See "Preparing for client installation" on page 125.

Installing an unmanaged client

Unmanaged clients do not connect to Symantec Endpoint Protection Manager. In most cases, unmanaged clients connect to your network intermittently or not at all.

You or the primary computer users must maintain the computers. This maintenance includes monitoring and adjusting the protection on the computers, and updating security policies, virus definitions, and software.

See "About managed and unmanaged clients" on page 146.

To install an unmanaged Windows client

1   On the computer, insert the product disc.

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

    If you downloaded the product, extract the entire product disc image to a physical disc, such as a hard disk. Run Setup.exe from the physical disc.

    If you exported the unmanaged client from the management console, copy the exported folder to the client computer, and then double-click Setup.exe.

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

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

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

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

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

    See "About the client installation settings" on page 141.

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

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

To install an unmanaged Mac client

1   On the Mac computer, insert and double-click the product disc.

    If you downloaded the product, extract the entire product disc image to a physical disc, such as a hard disk, on a Windows computer. Copy the SEP_MAC folder to the desktop of the Mac computer.

2   Double-click the SEP_MAC folder.

3   Double-click Symantec Endpoint Protection.dmg to mount it as a virtual disc.

4   Double-click Symantec Endpoint Protection.pkg to launch the installation.

5   On the **Introduction** panel, click **Continue**.

6   On the **Software License Agreement** panel, click **Continue**, and then click **Agree**.

    You can print or save the license agreement for review.

7   Click **Install**, and then click **Continue Installation**.

Enter the password for the Mac administrative account when prompted.

8   On the **Summary** panel, click **Log Out**.

When you log back on to the Mac computer, LiveUpdate launches to update the definitions.

See "Preparing for client installation" on page 125.

Uninstalling the Windows client

You uninstall the Symantec Endpoint Protection client by using the appropriate Windows control panel, such as Add or Remove Programs.

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

See your Windows documentation for more information.

See "About client deployment methods" on page 131.

To uninstall the client

The text that you see depends on the operating system of the client computer.

1   On the client computer, on the **Start** menu, click **Control Panel** > **Add or Remove Programs** (or **Control Panel > Programs** > **Uninstall a program**).

2   In the **Add or Remove Programs** (or **Uninstall or change a program**) dialog box, click **Symantec Endpoint Protection**, and then click **Change**, **Remove** or **Uninstall**.

3   Follow the onscreen prompts to remove the client software.

If the standard Windows uninstall method fails, you may have to uninstall the client manually. For more information, see the knowledge base article: Methods for uninstalling Symantec Endpoint Protection.

Uninstalling the Mac client

You can uninstall the Symantec Endpoint Protection Mac client by using the Symantec Uninstaller that is included on the product disc in the SEP_MAC folder. Two files are provided in the .tgz archive file. Symantec Uninstaller is the actual Symantec Endpoint Protection Mac client uninstaller. SymantecUninstaller.pkg lets you install the Symantec Uninstaller onto the client computer. For example, you can install the Symantec Uninstaller to allow

an administrative user to uninstall the Symantec Endpoint Protection Mac client at a future time. Installing the Symantec Uninstaller onto the client computer does not uninstall the Symantec Endpoint Protection Mac client.

Note: After you uninstall the Symantec Endpoint Protection client, you are prompted to restart the client computer to complete the uninstallation. Make sure that the client computer users save their work or close all open applications first.

To uninstall the Mac client

1   Copy the Symantec Uninstaller `.tgz` archive file to the Mac client computer.

2   Double-click the file to extract the Symantec Uninstaller folder using `Archive Utility`.

3   Double-click `Symantec Uninstaller`.

4   In the **Delete** column, check the box in front of Symantec Endpoint Protection, and then click **Uninstall**.

5   Click **Uninstall** again to confirm, then authenticate with your Mac's administrative user name and password when prompted.

6   Click **Restart** to restart the Mac computer.

If the Symantec Uninstaller fails, you may have to use an alternate method to uninstall.

For more information, see the knowledge base article: Methods for uninstalling Symantec Endpoint Protection.

Managing client installation packages

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

You can 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. Typically, if you use Active Directory Group Policy Object, you do not choose to export to a single executable file.

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 AutoUpgrade feature. You do not
need to redeploy software with installation deployment tools.

Table 5-8 Client installation package-related tasks

Task	Description
Configure client installation packages	You can select specific client protection technologies to install and you can specify how the installation interacts with end-users. See "Configuring client installation package features" on page 142.
Export client installation packages	You can export packages for Symantec-managed clients, third-party managed clients, and unmanaged clients. See "Exporting client installation packages" on page 139.
Add client installation package updates	When Symantec sends you client installation package updates, you add them to the database to make them available for distribution from Symantec Endpoint Protection Manager. You can optionally export the packages during this procedure to make the package available for deployment to computers that do not have the client software. See "Adding client installation package updates" on page 152.
Upgrade clients in one or more groups	You can install the exported packages to computers one at a time, or deploy the exported files to multiple computers simultaneously. When Symantec provides updates to client installation packages, you first add them to a Symantec Endpoint Protection Manager and make them available for exporting. You do not, however, have to reinstall them with client deployment tools. The easiest way to update clients in groups with the latest software is to use the console to update the group that contains the clients. You should first update a group with a small number of test computers. See "Upgrading clients by using AutoUpgrade in Symantec Endpoint Protection" on page 173. You can also update clients with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings policy permits updates.

Table 5-8   Client installation package-related tasks *(continued)*

Task	Description
Delete client installation packages	You can delete older client installation packages to save disk space. However, these older client installation packages are sometimes used to build upgrade packages when using AutoUpgrade. This results in smaller downloads by clients.

See "Preparing for client installation" on page 125.

Adding client installation package updates

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

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

To add a client installation package update

1   Copy the package to a directory on the computer that runs the Symantec Endpoint Protection Manager.

2   In the console, click **Admin**, and then click **Install Packages**.

3   Under **Tasks**, click **Add a Client Install Package**.

4   In the **Add a Client Install Package** dialog box, type a name and a description for the package.

5   Click **Browse**.

6   In the **Select Folder** dialog box, locate and select the *product_name*.info file for the new package, and then click **Select**.

7   When the **Completed successfully** prompt appears, do one of the following:

■ If you do not want to export the installation files and make them available for deployment, click **Close**.
You are finished with this procedure.

■ If you do want to export the installation files and make them available for deployment, click **Export this Package**, and then complete this procedure.

8 In the **Export Package** dialog box, click **Browse**.

9 In the **Select Export Folder** dialog box, browse to and select the directory to contain the exported package, and then click **OK**.

10 In the **Export Package** dialog box, select a group, and then set the other options according to your installation goals.

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

11 Click **OK**.

See "Managing client installation packages" on page 150.

See "Preparing for client installation" on page 125.

Chapter **6**

Upgrading Symantec Endpoint Protection

This chapter includes the following topics:

- Upgrading to a new release of Symantec Endpoint Protection

- Upgrade resources for Symantec Endpoint Protection 12.1

- Feature mapping between 11.x and 12.1 clients

- Supported Symantec Endpoint Protection Manager upgrade paths

- Increasing Symantec Endpoint Protection Manager disk space before upgrading to version 12.1

- Upgrading a management server

- Upgrading an environment that uses multiple embedded databases and management servers

- Turning off replication before upgrade

- Turning on replication after upgrade

- Stopping and starting the management server service

- Supported upgrade paths for the Symantec Endpoint Protection client

- About upgrading client software

- Upgrading clients by using AutoUpgrade in Symantec Endpoint Protection

- Updating client software with a LiveUpdate Settings policy

- Upgrading Group Update Providers

Upgrading to a new release of Symantec Endpoint Protection

You can upgrade to the newest release of the product to take advantage of new features. To install a new version of the software, you must perform certain tasks to ensure a successful upgrade or migration. You should also check the Known Issues that appear in the Release Notes for any late-breaking information relating to upgrades.

Before you upgrade, review the following information:

- System requirements
  For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

- New features in this version
  See "What's new in Symantec Endpoint Protection 12.1.2" on page 42.

- Feature changes between the previous version and the newest version of the client
  See "Feature mapping between 11.x and 12.1 clients" on page 161.

- Compatible Symantec Endpoint Protection Manager upgrade paths
  See "Supported Symantec Endpoint Protection Manager upgrade paths" on page 164.

- Compatible Windows client upgrade paths
  See "Supported upgrade paths for the Symantec Endpoint Protection client" on page 171.

- Compatible Mac client migrations
  See "Supported and unsupported migration paths for the Mac client" on page 181.

Table 6-1 displays the steps you need to perform to upgrade to the latest version.

This section is specific to upgrading the software in environments where a compatible version of Symantec Endpoint Protection or Symantec Network Access Control is already installed.

Note: If you upgrade from 11.x and use Application and Device Control, you must disable the Application Control rule "Protect client files and registry keys." After the clients receive the new policy, you may upgrade the client computers.

See "Creating a custom rule set and adding rules" on page 491.

Table 6-1 Process for upgrading to the full version

Step	Action	Description
Step 1	Back up the database	Back up the database that Symantec Endpoint Protection Manager uses to ensure the integrity of your client information. See "Backing up the database and logs" on page 744.
Step 2	Turn off replication	Turn off replication on all sites that are configured as replication partners to avoid any attempts to update the database during the installation. See "Turning off replication before upgrade" on page 168.
Step 3	If you have Symantec Network Access Control installed, enable local authentication	Enforcers are not able to authenticate clients during an upgrade. To avoid problems with client authentication, Symantec recommends that you enable local authentication before you upgrade. After the upgrade is finished, you can return to your previous authentication setting. See "Enabling local authentication on the Integrated Enforcer" on page 1015. See "Enabling local authentication on a Gateway Enforcer appliance" on page 904. See "Enabling local authentication on the LAN Enforcer appliance" on page 959.
Step 4	Stop the Symantec Endpoint Protection Manager service	You must stop the management server service before you install a newer version. See "Stopping and starting the management server service" on page 170.
Step 5	Upgrade the Symantec Endpoint Protection Manager software	Install the new version of the Symantec Endpoint Protection Manager on all sites in your network. The existing version is detected automatically, and all settings are saved during the upgrade. See "Installing Symantec Endpoint Protection Manager" on page 95.
Step 6	Turn on replication after the upgrade	Turn on replication when the installation is complete to restore your configuration. See "Turning on replication after upgrade" on page 169.

	Table 6-1	Process for upgrading to the full version *(continued)*

Step	Action	Description
Step 7	Upgrade Symantec client software	Upgrade your client software to the latest version.
		See "About upgrading client software" on page 172.
		See "Upgrading Group Update Providers" on page 175.
		When Symantec provides updates to client installation packages, you add the updates to a Symantec Endpoint Protection Manager and make them available for exporting. You do not, however, have to reinstall the client with client-deployment tools. The easiest way to update clients in groups with the latest software is to use AutoUpgrade. You should first update a group with a small number of test computers before you update your entire production network.
		See "Upgrading clients by using AutoUpgrade in Symantec Endpoint Protection" on page 173.
		You can also update clients with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings policy permits
		See "Managing content updates" on page 546.

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

Upgrade resources for Symantec Endpoint Protection 12.1

Table 6-2 lists the topics that help you prepare for a successful upgrade to the newest version.

Table 6-2   Product upgrade tasks and resources

Task	Resource
Learn about the Symantec Endpoint Protection 12.1 upgrade requirements	Before you upgrade, review the prerequisites, differences from previous versions, and supported upgrade paths.
	For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control
	Known issues for Symantec Endpoint Protection 12.1
	See "Feature mapping between 11.x and 12.1 clients" on page 161.
	See "Supported upgrade paths for the Symantec Endpoint Protection client" on page 171.
	See "Supported Symantec Endpoint Protection Manager upgrade paths" on page 164.
	See "Supported and unsupported migration paths for the Mac client" on page 181.
Upgrade Symantec Endpoint Protection Manager	Perform the following tasks before you upgrade the management server:
	■ Back up the database. See "Backing up the database and logs" on page 744. ■ Turn off replication (if used). See "Turning off replication before upgrade" on page 168. ■ Remove any packages that are assigned to the client groups. If you deploy the client packages that do not use the **Maintain existing client features when upgrading** option, these packages must be removed. For more information, see the knowledge base article Clients show "No Symantec protection technologies are installed" after migrating the SEPM from 11.x to 12.1

Table 6-2   Product upgrade tasks and resources *(continued)*

Task	Resource
Manage product licenses	Symantec Endpoint Protection 12.1 is licensed according to the number of clients that are needed to protect the computers at your site.
	See "Product license requirements" on page 82.
	See "About product upgrades and licenses" on page 118.
Upgrade client software	Prepare the computers that need a client upgrade. If you use Group Update Providers, they must be upgraded first.
	Note: When you upgrade from Symantec Endpoint Protection Small Business Edition, your upgrade license activates new features on previously installed clients.
	See "Preparing for client installation" on page 125.
	See "Upgrading Group Update Providers" on page 175.
	See "Upgrading clients by using AutoUpgrade in Symantec Endpoint Protection" on page 173.
	See "About client deployment methods" on page 131.

Table 6-3 provides additional information to upgrade.

Table 6-3   Additional upgrade resources

Item	Resource
Client installation package settings and features	You can configure client installation packages with a variety of settings and protection features.
	See "The types of security policies" on page 293.
	See "Client protection features by platform" on page 1083.
	See "About the client installation settings" on page 141.
	See "Configuring client installation package features" on page 142.
	See "Which features should you install on the client?" on page 132.
Feature and policy descriptions	See "About the types of threat protection that Symantec Endpoint Protection provides" on page 46.

Table 6-3   Additional upgrade resources *(continued)*

Item	Resource
Feature dependencies	See "How Symantec Endpoint Protection policy features work together" on page 356.

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

Feature mapping between 11.x and 12.1 clients

When you upgrade clients using the AutoUpgrade feature and check the **Maintain Existing Features** option, the features that are configured in legacy clients are mapped to the new version.

The tables in this section depict the feature mapping between previous versions and the new version of Symantec Endpoint Protection for common update scenarios.

If you migrate from a previous version, be aware that **Antivirus and Antispyware Protection** in Symantec Endpoint Protection 11.x is called **Virus and Spyware Protection** in version 12.1.

Table 6-4 compares the default protection technologies between 11.x and 12.1 clients.

Table 6-4   11.x to 12.1 default client protection

Default 11.x client protection	Default 12.1 client protection
Antivirus + TruScan	Antivirus + SONAR + Download Insight
Antivirus	Antivirus + Basic Download Insight
Antivirus without Proactive Threat Protection	Antivirus without SONAR or Download Insight

Table 6-5   11.x to 12.1 full protection

Existing 11.x features installed	12.1 features installed after AutoUpgrade
Antivirus and Antispyware Protection ■ Antivirus and Antispyware Protection	Virus and Spyware Protection ■ Basic Virus and Spyware Protection ■ Download Insight

Table 6-5   11.x to 12.1 full protection *(continued)*

Existing 11.x features installed	12.1 features installed after AutoUpgrade
Auto-Protect Email Protection ■ POP3/SMTP Scanner ■ Microsoft Outlook Scanner ■ Lotus Notes Scanner	Auto-Protect Email Protection ■ POP3/SMTP Scanner ■ Microsoft Outlook Scanner ■ Lotus Notes Scanner
Proactive Threat Protection ■ TruScan proactive threat scan ■ Application and Device Control	Proactive Threat Protection ■ SONAR ■ Application and Device Control
Network Threat Protection ■ Network Threat Protection ■ Intrusion Prevention	Network Threat Protection ■ Network Threat Protection ■ Intrusion Prevention

Table 6-6   11.x to 12.1 antivirus only

Existing 11.x features installed	12.1 features installed after AutoUpgrade
Antivirus and Antispyware Protection ■ Antivirus and Antispyware Protection	Virus and Spyware Protection ■ Basic Virus and Spyware Protection
Auto-Protect Email Protection ■ POP3/SMTP Scanner ■ Microsoft Outlook Scanner ■ Lotus Notes Scanner	Auto-Protect Email Protection ■ POP3/SMTP Scanner ■ Microsoft Outlook Scanner ■ Lotus Notes Scanner

Table 6-7   11.x to 12.1 antivirus + Proactive Threat Protection

Existing 11.x features installed	12.1 features installed after AutoUpgrade
Antivirus and Antispyware Protection ■ Antivirus and Antispyware Protection	Virus and Spyware Protection ■ Basic Virus and Spyware Protection ■ Download Insight

Table 6-7   11.x to 12.1 antivirus + Proactive Threat Protection *(continued)*

Existing 11.x features installed	12.1 features installed after AutoUpgrade
Auto-Protect Email Protection ■ POP3/SMTP Scanner ■ Microsoft Outlook Scanner ■ Lotus Notes Scanner	Auto-Protect Email Protection ■ POP3/SMTP Scanner ■ Microsoft Outlook Scanner ■ Lotus Notes Scanner
Proactive Threat Protection ■ TruScan proactive threat scan ■ Application and Device Control	Proactive Threat Protection ■ SONAR ■ Application and Device Control
Network Threat Protection ■ Intrusion Prevention	Network Threat Protection ■ Intrusion Prevention

Table 6-8   11.x to 12.1 (enterprise version) firewall only

Existing 11.x features installed	12.1 features installed after AutoUpgrade
Auto-Protect Email Protection ■ POP3/SMTP Scanner ■ Microsoft Outlook Scanner ■ Lotus Notes Scanner	Auto-Protect Email Protection ■ POP3/SMTP Scanner ■ Microsoft Outlook Scanner ■ Lotus Notes Scanner
Proactive Threat Protection ■ Application and Device Control	Proactive Threat Protection ■ Application and Device Control
Network Threat Protection ■ Network Threat Protection	Network Threat Protection ■ Network Threat Protection **Note:** The 12.1 version only includes the firewall

Table 6-9   12.0 Small Business Edition to 12.1 (enterprise version)

Existing 12.0 Small Business Edition features installed	12.1 features installed after AutoUpgrade
Virus and Spyware Protection ■ Virus and Spyware Protection	Virus and Spyware Protection ■ Basic Virus and Spyware Protection ■ Download Insight

Table 6-9   12.0 Small Business Edition to 12.1 (enterprise version) *(continued)*

Existing 12.0 Small Business Edition features installed	12.1 features installed after AutoUpgrade
Auto-Protect Email Protection ■ POP3/SMTP Scanner ■ Microsoft Outlook Scanner	Auto-Protect Email Protection ■ POP3/SMTP Scanner ■ Microsoft Outlook Scanner
Proactive Threat Protection ■ TruScan proactive threat scan	Proactive Threat Protection ■ SONAR ■ Application and Device Control
Network Threat Protection ■ Firewall and Intrusion Prevention	Network Threat Protection ■ Network Threat Protection ■ Intrusion Prevention

Supported Symantec Endpoint Protection Manager upgrade paths

The following Symantec Endpoint Protection Manager upgrade paths are supported:

■ From 11.x to 12.1.2 (enterprise version)

■ From 12.0 Small Business Edition to 12.1.2 (enterprise version)

■ From 12.1 Small Business Edition to 12.1.2 (enterprise version)

Note: Symantec AntiVirus 10.x server information can be imported during the installation of Symantec Endpoint Protection Manager version 12.1.2.

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

The following downgrade paths are not supported:

■ Symantec Endpoint Protection 11.x to 12.1.2 Small Business Edition

■ 12.1.x (enterprise version) to 12.1.2 Small Business Edition

For details on upgrading from specific versions of Symantec Endpoint Protection Manager 11.x to 12.1, please see the following knowledge base article:

Supported upgrade paths to Symantec Endpoint Protection Manager 12.1 from Symantec Endpoint Protection Manager 11.x

Increasing Symantec Endpoint Protection Manager disk space before upgrading to version 12.1

The Symantec Endpoint Protection Manager version 12.1 requires a minimum amount of available disk space for the installation. Make sure that any legacy servers or new hardware meet the minimum hardware requirements. However, additional available disk space may be needed during an upgrade to allow for the creation of temporary files.

Note: Make a backup of the database before making configuration changes.

See "Backing up the database and logs" on page 744.

Table 6-10 lists ways you can make more disk space available for the upgrade.

Table 6-10 Tasks to increase disk space on the management server

Task	Description
Change the LiveUpdate settings to reduce space requirements.	1 Go to **Admin > Servers** and right-click on **Local Site**. Select **Edit Site Properties.**
	2 On the **LiveUpdate** tab, uncheck **Store client packages unzipped to provide better network performance for upgrades**.
	3 On the **LiveUpdate** tab, reduce the number of content revisions to keep. The optimum value is 30 revisions but a lower setting uses less disk space. For the upgrade, you can lower the setting to 10. Allow time for the Symantec Endpoint Protection Manager to purge the extra revisions. After the upgrade, return the setting to 30.
Make sure that unused virus definitions are deleted from the Symantec Endpoint Protection Manager database.	1 Go to **Admin > Servers** and right-click on **Local Site**. Select **Edit Properties**
	2 On the **Database** tab, make sure that **Delete unused virus definitions** is checked.

Table 6-10 Tasks to increase disk space on the management server *(continued)*

Task	Description
Relocate or remove co-existing programs and files	■ If other programs are installed on the same computer with the Symantec Endpoint Protection Manager, consider relocating them to another server. Unused programs can be removed. ■ If the Symantec Endpoint Protection Manager shares the computer with other storage intensive applications, consider dedicating a computer to support only the Symantec Endpoint Protection Manager. ■ Remove temporary Symantec Endpoint Protection files. For a list of temporary files that you can remove, see the knowledge base article, Symantec Endpoint Protection Manager directories contain many .TMP folders consuming large amounts of disk space. **Note:** Defragment the hard drive after removing programs and files.
Use an external database	If the Symantec Endpoint Protection database resides on the same computer with the Symantec Endpoint Protection Manager, consider installing a Microsoft SQL Server database on another computer. Significant disk space is saved and in most cases, performance is improved. See "About choosing a database type" on page 87.

Note: Make sure that the client computers also have enough disk space before an upgrade. Check the system requirements and as needed, remove unnecessary programs and files, and then defragment the client computer hard drive.

For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

Upgrading a management server

You must upgrade all management servers before you upgrade any clients.

If you upgrade management servers in an environment that supports load balancing, failover, or replication, you must prepare and upgrade them in a specific order.

Warning: You must follow the scenario that applies to your type of installation, or your upgrade can fail.

The upgrade process is similar to a fresh installation.

See "Setting up failover and load balancing" on page 737.

See "Upgrading an environment that uses multiple embedded databases and management servers" on page 168.

See "Setting up sites and replication" on page 187.

Table 6-11 lists the tasks to upgrade Symantec Endpoint Protection Manager.

Table 6-11   Upgrade tasks

Task	Description
Install and configure the new management server	Install the management server, and then configure it with the Management Server Configuration Wizard.
	To upgrade Symantec Sygate Enterprise Protection servers that use Host Integrity policies or Enforcer protection, install the management server for Symantec Endpoint Protection first. Then, you repeat the installation procedure and you install the management server for Symantec Network Access Control to gain access to the Host Integrity and Enforcer functionality.
	See "Installing Symantec Endpoint Protection Manager" on page 95.
Log onto the management server	When the Symantec Endpoint Protection Manager logon panel appears, log on to the console by using your legacy logon credentials.
	See "Logging on to the Symantec Endpoint Protection Manager console" on page 99.
(Optional) Install the management server for Symantec Network Access Control	Log off the Symantec Endpoint Protection Manager. Then repeat this process and install Symantec Endpoint Protection Manager for Symantec Network Access Control from the Symantec Network Access Control product disc.
	See "Upgrading Symantec Endpoint Protection Manager to include Symantec Network Access Control" on page 799.

Note: You are not required to restart the computer after the upgrade, but you may notice performance improvements if you restart the computer and log on.

Upgrading an environment that uses multiple embedded databases and management servers

Migrating an installation instance that uses multiple embedded database and management servers has the following implications:

■ No failover or load balancing is performed because the embedded database does not support failover or load balanced servers.

■ The management servers are configured for replication.

All sites have a computer on which you first installed the management server. Only one of these management servers was installed with a license and a preshared secret. You must migrate this management server first. You then migrate the other management servers that were installed for replication.

To upgrade an environment that uses multiple embedded databases and management servers

1 On all management servers, disable replication.

   See "Turning off replication before upgrade" on page 168.

2 Authenticate to and log on to the computer that contains the Symantec Endpoint Protection Manager that was installed with the license and preshared secret.

   Do not log on to the Symantec Endpoint Protection Manager.

3 Migrate the management server.

   See "Upgrading a management server" on page 166.

4 Migrate all additional management servers one by one.

5 After you migrate the servers, enable replication on each server.

   See "Turning on replication after upgrade" on page 169.

Turning off replication before upgrade

If you have legacy Symantec sites that are configured for replication, you must turn off replication before you upgrade. You do not want sites trying to replicate data between legacy and updated databases during or after the upgrade. You must

turn off replication at each site that replicates. You must log on to and turn off replication at a minimum of two sites.

See "Turning on replication after upgrade" on page 169.

To disable replication before upgrade

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

2   Under **Servers**, expand **Replication Partners** and select a site.

3   Right-click the site, and then click **Delete**.

4   Click **Yes**.

5   Log off the console, and then repeat this procedure at all sites that replicate data.

Turning on replication after upgrade

After you upgrade the servers that used replication, you must turn on replication. After migration, you add a replication partner to enable replication. You must add replication partners only on the computer on which you first installed the management server. Replication partners automatically appear on the other management servers.

See "Turning off replication before upgrade" on page 168.

See "Upgrading to a new release of Symantec Endpoint Protection" on page 156.

To turn on replication after upgrade

1   On the console, click **Admin > Servers**.

2   Under **Servers**, expand **Replication Partners** and select a site.

3   Right-click the site, and then click **Add Partner**.

4   In the **Add Replication Partner** panel, click **Next**.

5   In the **Remote Site Information** panel, enter the identifying information about the replication partner, enter the authentication information, and then click **Next**.

6   In the **Schedule Replication** panel, set the schedule for when replication occurs automatically, and then click **Next**.

7   In the **Replication of Log Files and Client Packages** panel, check the items to replicate, and then click **Next**.

     Package replication uses large amounts of traffic and hard disk space.

8 In the **Completing the Add Replication Partner Wizard** panel, click **Finish**.

9 Repeat this procedure for all computers that replicate data with this computer.

Stopping and starting the management server service

Before you upgrade, you must manually stop the Symantec Endpoint Protection Manager service on every management server in your site. After you upgrade, the service starts automatically.

Warning: If you do not stop the Symantec Endpoint Protection Manager service before you upgrade the server, you risk corrupting your existing Symantec Endpoint Protection database.

Note: If you stop the management server service, clients can no longer connect to it. If clients are required to communicate with the management server to connect to the network, they are denied access until the management server service is restarted.

For example, a client must communicate with the management server to pass a Host Integrity check.

See "Upgrading to a new release of Symantec Endpoint Protection" on page 156.

To stop the Symantec Endpoint Protection Manager service

1 Click **Start > Settings > Control Panel > Administrative Tools > Services**.

2 In the **Services** window, under **Name**, scroll to and right-click **Symantec Endpoint Protection Manager**.

3 Click **Stop**.

4 Close the Services window.

Warning: Close the Services window or your upgrade can fail.

---

5 Repeat this procedure for all installations of Symantec Endpoint Protection Manager.

Note: To start the Symantec Endpoint Protection Manager service, follow the above procedure and click **Start** instead of **Stop**.

To stop the Symantec Endpoint Protection Manager service using the command line

◆ From a command prompt, type:

```
net stop semsrv
```

To start the Symantec Endpoint Protection Manager service using the command line

◆ From a command prompt, type:

```
net start semsrv
```

Supported upgrade paths for the Symantec Endpoint Protection client

The following Symantec Endpoint Protection client versions can upgrade directly to version 12.1.2:

- 11.0.780.1109

- 11.0.1000.1375 - Maintenance Release 1 (MR1)

- 11.0.2000.1567 - Maintenance Release 2 (MR2), with or without maintenance patches

- 11.0.3001.2224 - Maintenance Release 3 (MR3)

- 11.0.4000.2295 - Maintenance Release 4 (MR4), with or without maintenance patches

- 11.0.5002.333 - Release Update 5 (RU5)

- 11.0.6000.550 - Release Update 6 (RU6), with or without maintenance patches

- 11.0.7000.975 - Release Update 7 (RU7), with or without maintenance patches

- 12.0.122.192 Small Business Edition

- 12.0.1001.95 Small Business Edition - Release Update 1 (RU1)

- 12.1.671.4971

- 12.1.1000.157 - Release Update 1 (RU1), with or without maintenance patches

The following downgrade paths are not supported:

- Symantec Endpoint Protection 11.x to 12.1 Small Business Edition

- 12.1.x (enterprise version) to 12.1.2 Small Business Edition

Migrating from Symantec AntiVirus 10.x to 12.1 is supported. Migrating from Symantec AntiVirus 9.x and Symantec Sygate Enterprise Protection 5.x is not supported.

See "Supported and unsupported migration paths to Symantec Endpoint Protection" on page 179.

About upgrading client software

You can use several methods to upgrade Symantec client software. Some methods can take up to 30 minutes. Therefore, you may want to upgrade client software when most users are not logged on to their computers.

Table 6-12   Methods to upgrade the client software

Upgrade method	Description
AutoUpgrade	Use AutoUpgrade to update clients in one or more groups from the Symantec Endpoint Protection Manager console. See "Upgrading clients by using AutoUpgrade in Symantec Endpoint Protection" on page 173.
LiveUpdate Settings policy	Configure a LiveUpdate Settings policy for a group that defines a LiveUpdate server and allows clients to run LiveUpdate to obtain product updates. See "Updating client software with a LiveUpdate Settings policy" on page 174.
Product disc	Use the installation program on the product disc to install a new version of the client.
Other methods	Use one of the other supported methods of installing client software. See "About client deployment methods" on page 131.

If the Symantec Network Access Control client is also installed, you should upgrade both the Symantec Endpoint Protection client and the Symantec Network Access Control client. You can assign both the Symantec Endpoint Protection package and the Symantec Network Access Control package to the same group. In this case, make sure that the Maintain Features option is selected.

See "Upgrading to a new release of Symantec Endpoint Protection" on page 156.

Upgrading clients by using AutoUpgrade in Symantec Endpoint Protection

The AutoUpgrade process lets you automatically upgrade the Symantec Endpoint Protection client software for all the clients that are contained in a group. For example, you can use AutoUpgrade to upgrade clients to a new release update or product version.

You must test the AutoUpgrade process before you attempt to upgrade a large number of clients in your production network. If you do not have a test network, you can create a test group within your production network. For this kind of test, you add a few non-critical clients to the test group and then upgrade them by using AutoUpgrade.

You confirm that the upgrade completed successfully by verifying the version number of the client software. The version number is displayed in the client's **Help > About** panel. The updated client version number is also displayed in the Symantec Endpoint Protection Manager on the **Clients** page after a successful check-in. You select the group, then the **Clients** tab, and change the view to **Client Status**.

Note: If you upgrade from 11.x and use Application and Device Control, you must disable the Application Control rule "Protect client files and registry keys." After the clients receive the new policy, you may upgrade using AutoUpgrade.

See "Creating a custom rule set and adding rules" on page 491.

See "About upgrading client software" on page 172.

To upgrade clients by using AutoUpgrade in Symantec Endpoint Protection

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

2 Click **Install Packages**.

3 Under **Tasks**, click **Upgrade Clients with Package**.

4 In the **Upgrade Clients Wizard** panel, click **Next**.

5 In the **Select Client Install Package** panel, select the appropriate client installation package, and then click **Next**.

6 In the **Specify Groups** panel, select the groups that contain the client computers that you want to upgrade, and then click **Next**.

7 In the **Package Upgrade Settings** panel, select **Download from the management server**.

   You can optionally stage and select a package on a Web server.

8   Click **Upgrade Settings**.

9   On the **General** tab, select **Maintain existing client features when updating**.

     You can optionally add or remove features when upgrading.

10   Optionally, on the **Notification** tab, customize the user notification settings. You can customize the message that is displayed on the client computer during the upgrade. You can also allow the user to postpone the upgrade by an amount you specify.

     For more information about schedule and notification settings, click **Help**.

11   Click **OK**.

12   In the **Upgrade Clients Wizard Complete** panel, click **Next**.

13   Click **Finish**.

Updating client software with a LiveUpdate Settings policy

You can update Symantec client product software automatically by permitting product updates with a LiveUpdate Settings policy. When product updates are permitted and an update is available, clients download and install them when a LiveUpdate session runs. The session can be scheduled or manually started. When the LiveUpdate policy is not configured to download product updates, client software can be only updated by using the Symantec Endpoint Protection Manager console or manually.

By default, when the Symantec Endpoint Protection Manager downloads and processes content through LiveUpdate, it is configured to download client updates. When the management server downloads a new client version, you can select the new package and upgrade clients with AutoUpgrade or with another upgrade method.

See "About upgrading client software" on page 172.

See "Upgrading clients by using AutoUpgrade in Symantec Endpoint Protection" on page 173.

See "Managing content updates" on page 546.

To update Symantec client software with a LiveUpdate Settings policy

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

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

3   In the right pane, on the **LiveUpdate Settings** tab, click a LiveUpdate policy.

4   In the lower portion of the left pane, under **Tasks**, click **Edit the Policy**.

5   Under **LiveUpdate Policy**, click **Advanced Settings**.

6   In the **Advanced Settings** pane, under **Product Update Settings**, check
    **Download Symantec Endpoint Protection product updates using a
    LiveUpdate server**.

7   Click **OK**, and then apply the policy to a group or a location in a group.

See "Performing the tasks that are common to all policies" on page 290.

Upgrading Group Update Providers

Use this procedure to upgrade clients that are Group Update Providers.

See "Upgrading to a new release of Symantec Endpoint Protection" on page 156.

To upgrade Group Update Provider clients

1   Upgrade the Symantec Endpoint Protection Manager server to the new version
    of the software.

2   Upgrade the clients that are Group Update Providers to the new version of
    the client software.

3   Update the rest of the clients to the new version of the client software.

Migrating to Symantec Endpoint Protection

This chapter includes the following topics:

- Migrating from Symantec AntiVirus or Symantec Client Security

- Supported and unsupported migration paths to Symantec Endpoint Protection

- Supported and unsupported migration paths for the Mac client

- Disabling scheduled scans in Symantec System Center

- Disabling LiveUpdate in Symantec System Center

- Turning off the roaming service in Symantec System Center

- Unlocking server groups in Symantec System Center

- Turning off Tamper Protection in Symantec System Center

- Uninstalling and deleting reporting servers

- About computer groups imported with the Migration Wizard

- Importing group settings and policy settings with the Migration Wizard

Migrating from Symantec AntiVirus or Symantec Client Security

You can migrate the groups, the clients, and the settings from a Symantec legacy virus protection software environment. During migration, the group data and policy data from the legacy installation populates the database in Symantec Endpoint Protection. You then deploy installation packages to the migrated clients.

Note: Management servers migrate the legacy clients.

See "Supported and unsupported migration paths to Symantec Endpoint Protection" on page 179.

Table 7-1   Migration summary

Task	Description
Prepare for legacy migration from within the Symantec System Center	Perform the following tasks to prepare your legacy installation for migration: ■ Disable scheduled scans. The migration might fail if a scan is running during migration. See "Disabling scheduled scans in Symantec System Center" on page 181. ■ Disable LiveUpdate. Conflicts might occur if LiveUpdate runs on the client computers during migration. See "Disabling LiveUpdate in Symantec System Center" on page 182. ■ Turn off roaming service. Migration might hang and fail to complete if the roaming service is running on the client computers. See "Turning off the roaming service in Symantec System Center" on page 182. ■ Unlock server groups. You may encounter unpredictable results if you migrate from Symantec AntiVirus before you unlock the server groups. See "Unlocking server groups in Symantec System Center" on page 183. ■ Turn off Tamper Protection. Tamper Protection can cause unpredictable results during migration. See "Turning off Tamper Protection in Symantec System Center" on page 184. ■ Uninstall and delete reporting servers. Uninstall the reporting servers, and optionally delete the database files. See "Uninstalling and deleting reporting servers" on page 184. For additional technical information, see your Symantec legacy virus protection software documentation on the following product pages: ■ Symantec AntiVirus Corporate Edition ■ Symantec Client Security

Table 7-1   Migration summary *(continued)*

Task	Description
Install the Symantec Endpoint Protection Manager, and migrate legacy group and policy settings when prompted	Use the Migration Wizard to import the legacy group settings and policy settings from your Symantec AntiVirus server. The Migration Wizard appears after you install and configure the management console. You can also click **Start Menu** > **All Programs** > **Symantec Endpoint Protection Manager** > **Symantec Endpoint Protection Manager Tools** > **Migration Wizard**.
	See "Installing Symantec Endpoint Protection Manager" on page 95.
	You can also adjust the migrated group settings and policy settings after you import them.
	See "About computer groups imported with the Migration Wizard" on page 185.
	See "Importing group settings and policy settings with the Migration Wizard" on page 185.
	See "Moving a client computer to another group" on page 219.
	For more information on how to perform common tasks between the Symantec System Center and Symantec Endpoint Protection Manager, see: Symantec Endpoint Protection Manager 12.1.x reference guide for Symantec System Center users
Deploy the Symantec Endpoint Protection client software	Deploy the client to the new client computers.
	See "About client deployment methods" on page 131.
Perform post-migration tasks	Familiarize yourself with the interface, features, and functions of Symantec Endpoint Protection. You can perform many of the same tasks that are done after a new installation to become familiar with Symantec Endpoint Protection Manager.
	See "Getting up and running on Symantec Endpoint Protection for the first time" on page 51.

See "Upgrade resources for Symantec Endpoint Protection 12.1" on page 158.

Supported and unsupported migration paths to Symantec Endpoint Protection

Symantec Endpoint Protection detects and migrates Symantec legacy virus protection software.

Table 7-2   Supported and unsupported migration paths

Product	Description
Symantec legacy virus protection software	You can migrate Symantec legacy virus protection software to Symantec Endpoint Protection.
	Migration detects and migrates installations of the following Symantec legacy virus protection software:
	■ Symantec AntiVirus Corporate Edition 10.x ■ Symantec Client Security 3.x ■ Symantec AntiVirus for Mac (client only)
	Migration from the following legacy products are not supported:
	■ Symantec AntiVirus 9.x or earlier ■ Symantec Client Security 2.x ■ Symantec Sygate Enterprise Protection 5.x
	You may skip migration as follows:
	■ Uninstall the Symantec legacy virus protection software from your servers and client computers. ■ During Symantec Endpoint Protection Manager installation, do not select the migration option. ■ After initial product installation, use Symantec Endpoint Protection Manager to adjust the group settings and policy settings. ■ Install the Symantec Endpoint Protection client on the unprotected legacy computers.
	See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.
	See "Supported and unsupported migration paths for the Mac client" on page 181.
Symantec Endpoint Protection	You can upgrade Symantec Endpoint Protection from Symantec Endpoint Protection 11.x or Small Business Edition 12.0, or to a new release update of 12.1.
	See "Upgrading to a new release of Symantec Endpoint Protection" on page 156.
	See "Supported upgrade paths for the Symantec Endpoint Protection client" on page 171.

See "Upgrade resources for Symantec Endpoint Protection 12.1" on page 158.

Supported and unsupported migration paths for the Mac client

Table 7-3 displays the products that can be migrated to the Symantec Endpoint Protection for Mac client.

Table 7-3   Migration paths from Symantec AntiVirus for Mac to the Symantec Endpoint Protection Mac client

Migrate from	Migrate to	Supported?
Managed Symantec AntiVirus for Mac client	Managed Symantec Endpoint Protection for Mac client	Yes
Unmanaged Symantec AntiVirus for Mac client	Unmanaged Symantec Endpoint Protection for Mac client	Yes
Unmanaged Symantec AntiVirus for Mac client	Managed Symantec Endpoint Protection for Mac client	Yes
Managed Symantec AntiVirus for Mac client	Unmanaged Symantec Endpoint Protection for Mac client	Yes, but managed client settings are retained.
Norton AntiVirus for Mac	Managed or unmanaged Symantec Endpoint Protection for Mac client	No. Client must uninstall Norton products before installing Symantec Endpoint Protection.

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

Disabling scheduled scans in Symantec System Center

If a scan is scheduled to run and is running while the client migration occurs, migration may fail. A best practice is to disable scheduled scans during migration and then enable after migration.

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

To disable scheduled scans in Symantec System Center

1   In the Symantec System Center, do one of the following actions:

■ Right-click a management server.

- ■ Right-click a client group.

2 Click **All Tasks > Symantec AntiVirus > Scheduled Scans**.

3 In the Scheduled Scans dialog box, on the Server Scans tab, uncheck all scheduled scans.

4 On the Client Scans tab, uncheck all scheduled scans, and then click **OK**.

5 Repeat this procedure for all primary management servers, secondary management servers, and all client groups.

Disabling LiveUpdate in Symantec System Center

If LiveUpdate runs on client computers during migration, conflicts may occur. Therefore, you must turn off LiveUpdate on client computers during migration.

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

To disable LiveUpdate in Symantec System Center

1 In the Symantec System Center, right-click a server group.

2 Click **All Tasks > Symantec AntiVirus > Virus Definition Manager**.

3 In the Virus Definition Manager dialog box, check **Update only the primary server of this server group**, and then click **Configure**.

4 In the Configure Primary Server Updates dialog box, uncheck **Schedule for Automatic Updates**, and then click **OK**.

5 In the Virus Definition Manager dialog box, uncheck the following selections:

- ■ **Update virus definitions from parent server**

- ■ **Schedule client for automatic updates using LiveUpdate**

- ■ **Enable continuous LiveUpdate**

6 Check **Do not allow client to manually launch LiveUpdate**, and then click **OK**.

7 Repeat this procedure for all server groups if you have more than one.

Turning off the roaming service in Symantec System Center

If the roaming service is running on client computers, the migration might hang and fail to complete. If the roaming service is turned on, you must turn it off before starting the migration.

> **Note:** If your roaming clients run Symantec AntiVirus version 10.x, you must unlock your server groups before you disable the roaming service. This practice helps ensure that roaming clients are properly authenticated with certificates to their parent server.

To turn off the roaming service in Symantec System Center

1   In the Symantec System Center, right-click a server group.

2   Click **All Tasks > Symantec AntiVirus > Client Roaming Options**.

3   In the Client Roaming Options dialog box, in the Validate parent every minutes box, type **1**.

4   In the Search for the nearest parent every minutes box, type **1**, and then press **OK**.

5   Wait a few minutes.

6   In the Symantec System Center, right-click a server group.

7   Click **All Tasks > Symantec AntiVirus > Client Roaming Options**.

8   In the Client Roaming Options dialog box, uncheck **Enable roaming on clients that have the Symantec AntiVirus Roaming service installed**.

9   Click **OK**.

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

Unlocking server groups in Symantec System Center

If you do not unlock server groups before migration, unpredictable results may occur. Also, if the roaming service is enabled for clients, the unlocking the server group helps ensure that the clients properly authenticate to a parent server. Clients that properly authenticate to a parent server get placed in the database. Clients that get placed in the database automatically appear in the correct legacy group in the console after installation.

To unlock a server group

1   In the Symantec System Center, right-click a locked server group, and then click **Unlock Server Group**.

2   In the **Unlock Server Group** dialog box, type the authentication credentials if necessary, and then click **OK**.

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

Turning off Tamper Protection in Symantec System Center

Tamper Protection prevents processes from interfering with Symantec processes. You should turn off Tamper Protection before migration. Tamper Protection can cause unpredictable results during migration.

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

To turn off Tamper Protection in Symantec System Center

1   In the Symantec System Center, do one of the following actions:

   ■   Right-click a server or server group, and then click **All Tasks > Symantec AntiVirus > Client Tamper Protection Options**.

   ■   Right-click a server or server group, and then click **All Tasks > Symantec AntiVirus > Server Tamper Protection Options**.

2   If you use Symantec AntiVirus 10.1, under **Protection**, uncheck **Processes** and then uncheck **Internal Objects**.

3   Uncheck **Enable Tamper Protection**.

4   If you configure **Client Tamper Protection Options**, you can click **Reset All**. This option propagates the settings on this tab to every client that is attached to the server or server group.

Uninstalling and deleting reporting servers

If you installed one or more reporting servers, you must uninstall these reporting servers, and optionally delete the database files. You must also delete reporting servers from the Symantec System Center. Complete reporting server uninstallation information is available in the Symantec System Center Online Help. Legacy settings were stored in the Windows registry. All settings are now stored in a database along with the reporting data.

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

To uninstall reporting servers

1   Log on to a computer that runs the reporting server.

2   Click **Start > Settings > Control Panel > Add or Remove Programs**.

3   In the Add or Remove Programs dialog box, click **Symantec Reporting Server**, and then click **Remove**.

4   Follow the on-screen prompts until you delete the reporting server.

5   Repeat this procedure for all reporting servers.

To delete reporting servers from the Symantec System Center

1   In the Symantec System Center, right-click and expand **Reporting**.

2   Right-click each reporting server, and then click **Delete**.

About computer groups imported with the Migration Wizard

You import computer groups from Symantec AntiVirus or Symantec Client Security with the Migration Wizard. The wizard creates a **My Company** child group for each imported legacy group. The **My Company** child group name is a concatenation of each legacy group and its legacy child groups.

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

See "Importing group settings and policy settings with the Migration Wizard" on page 185.

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

Importing group settings and policy settings with the Migration Wizard

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

You can run the Migration Wizard during initial product installation. You can also run the Migration Wizard from the **Start** menu on the computer that hosts Symantec Endpoint Protection Manager.

To import group settings and policy settings with the Migration Wizard

1   Start the Migration Wizard if necessary.

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

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

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

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

4 Click **Next**.

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

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

6 Click **Next**.

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

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

Managing sites and replication

This chapter includes the following topics:

- Setting up sites and replication
- About determining how many sites you need
- How replication works
- Replicating data on demand
- Changing the automatic replication schedule
- Specifying which data to replicate
- Deleting replication partners
- Re-adding a replication partner that you previously deleted

Setting up sites and replication

A site consists of one database, one or more management servers, and clients. By default, you deploy Symantec Endpoint Protection with a single site. Organizations with more than one datacenter or physical location generally use multiple sites.

Table 8-1 displays the steps to follow to set up additional sites and replication.

| Table 8-1 | | Process for setting up sites |

Steps	Tasks	Description
Step 1	Determine whether you need to add another site.	Before you set up multiple sites and replication, make sure that it is necessary. Symantec recommends that you set up replication only in specific circumstances. If you do add an additional site, decide which site design works for your organization. See "About determining how many sites you need" on page 189. For more information on whether or not to set up replication, see the following knowledge base article: When to use replication with Symantec Endpoint Protection Manager See "How replication works" on page 191.
Step 2	Install Symantec Endpoint Protection Manager on the first site.	When you install Symantec Endpoint Protection for the first time, by default you have installed the first site, or the local site. See "Installing Symantec Endpoint Protection Manager" on page 95.
Step 3	Install Symantec Endpoint Protection Manager on the second site.	You install the management server for the second site by using the **Management Server Configuration** wizard. In the wizard, click the **Install an additional site** option and following the instructions in the wizard. The second management server is classified as a remote site and called a replication partner. When you add the second site as a replication partner, you perform the following tasks: ■ By default, replication is scheduled to occur automatically. However, you can change the replication schedule, based on the amount of disk space that is available. See "Changing the automatic replication schedule" on page 195. ■ Choose whether to replicate logs, client installation packages, or LiveUpdate content. See "Specifying which data to replicate" on page 196. Symantec recommends that you add a maximum of five sites in the site farm. For information on how to set up replication, see the following video: Replication Concepts and Configuration

	Table 8-1	Process for setting up sites *(continued)*

Steps	Tasks	Description
Step 4	Replicate the data between the two sites	The first time that the databases between the two sites replicate, let the replication finish completely. The replication may take a long time because the entire database gets replicated.
		You may want to replicate the data immediately, rather than waiting until the database are scheduled to replicate. You can also change the replication schedule to occur earlier or later.
		See "Replicating data on demand" on page 194.
		See "Changing the automatic replication schedule" on page 195.

After you configure the Symantec Endpoint Protection, you should back up the database, which contains all your configuration changes.

If you delete a replication partner to migrate or upgrade to the latest version of the management server, you must re-add the replication partner.

See "Backing up the database and logs" on page 744.

See "Deleting replication partners" on page 196.

See "Re-adding a replication partner that you previously deleted" on page 197.

See "Connecting to a directory server on a replicated site" on page 215.

About determining how many sites you need

A majority of small and medium-sized organizations need only a single site to centrally manage network security. Since each site has only one database, all data is centrally located.

Even a large organization with a single geographic location typically needs only needs one site. But for the organizations that are too complex to manage centrally, you should use a distributed management architecture with multiple sites.

You should consider multiple sites for any of the following factors:

■ A large number of clients.

■ The number of geographical locations and the type of communications links between them.

■ The number of functional divisions or administrative groups.

■ The number of datacenters. A best practice is to set up one Symantec Endpoint Protection site for each datacenter.

■ How frequently you want to update the content.

■ How much client log data you need to retain, how long you need to retain it, and where it should be stored.

■ A slow WAN link between multiple physical locations with thousands of clients. If you set up a second site with its own management server, you can minimize the client-server traffic over that slow link. With fewer clients, you should use a Group Update Provider.
See "Using Group Update Providers to distribute content to clients " on page 580.

■ Any miscellaneous corporate management and IT security management considerations that are unique.

Use the following size guidelines to decide how many sites to install:

■ Install as few sites as possible, up to a maximum of 20 sites. You should keep the number of replicated sites under five.

■ Connect up to 10 management servers to a database.

■ Connect up to 45,000 to 50,000 clients to a management server.

After you add a site, you should duplicate site information across multiple sites by replication. Replication is the process of sharing information between databases to ensure that the content is consistent.

Table 8-2 displays the multi-site designs you can choose from.

Table 8-2   Multi-site designs

Site design	Description
Distributed	Each site performs replication bi-directionally for groups and policies, but not logs and content. To view the site reports, you use the console to connect to a management server in the remote site.
	Use this design when you do not need immediate access to remote site data.
Centralized logging	All logs are forwarded from the other sites to a central site.
	Use this design when you require centralized reporting.

Table 8-2   Multi-site designs *(continued)*

Site design	Description
High availability	Each site has multiple management server installations and database clustering. You can configure client computers to automatically switch to an alternative management server if the primary management server becomes unavailable.
	Use this design to provide redundancy, failover, and disaster recovery.
	Note: When you use replication with an embedded database, Symantec recommends that you do not add load balancing, as data inconsistency and loss may result.
	See "Setting up failover and load balancing" on page 737.

Note: Do not add sites to handle additional clients. Instead, you can install two or more management servers and use the management server list.

For more information on whether or not to set up replication, see the following knowledge base article: When to use replication with Symantec Endpoint Protection Manager

See "How replication works" on page 191.

See "Setting up sites and replication" on page 187.

See "Managing content updates" on page 546.

How replication works

Replication enables data to be duplicated between databases on separate sites so that both databases contain the same information. If one database fails, you can manage each site by using the information on the database from the second site.

A partner is a management server on another site with a different management server and database. A site may have as many partners as needed. Each partner, or remote site, connects to the main site or local site, which is the site that you are logged on to. All sites that are set up as partners are considered to be in the same site farm.

Each site you replicate data with is either a replication partner or a site partner. Both replication partners and site partners use multiple management servers, but the database they use and the way in which they communicate is different:

■ Replication partners can use either an embedded database or a Microsoft SQL Server database. The management servers do not share the database. All replication partners share a common license key.
If you use an embedded database, you can only connect one Symantec Endpoint Protection Manager. If you use the Microsoft SQL Server database, you can connect multiple management servers that share one database. Only one of the management servers needs to be set up as a replication partner.

■ Site partners share a single Microsoft SQL Server database.

The changes that you make on any partner are duplicated to all other partners. For example, you may want to set up one site at your main office (site 1) and a second site (site 2). Site 2 is a partner to site 1. The databases on site 1 and site 2 are reconciled by using the replication schedule. If a change is made on site 1, it automatically appears on site 2 after replication occurs. If a change is made on site 2, it automatically appears on site 1 after replication occurs. You can also install a third site (site 3) that can replicate data from either site 1 or site 2.

After replication occurs, the database on site 1 and the database on site 2 are the same. Only computer identification information for the servers differs.

Groups and policies are always replicated. You can choose to replicate logs, updated content, and patches.

Figure 8-1   How replication works between the main site and two remote sites
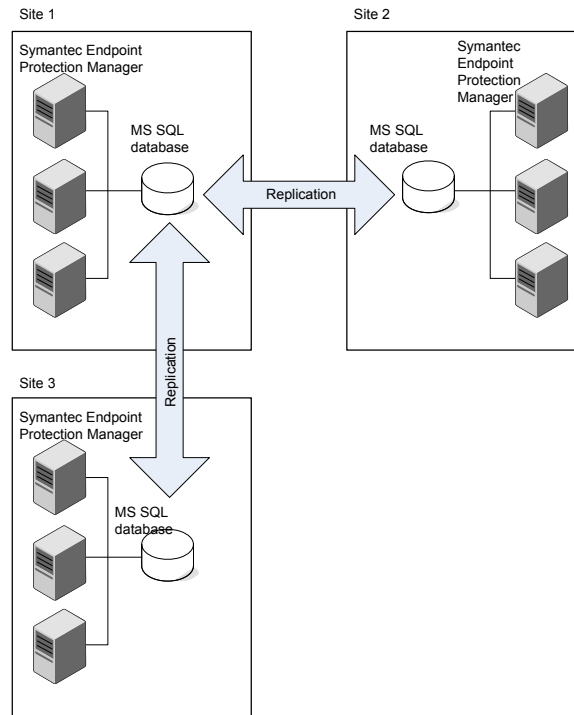
See "How to resolve data conflicts between sites during replication" on page 193.

See "Specifying which data to replicate" on page 196.

See "About determining how many sites you need" on page 189.

For more information on how often to replicate, see the following knowledge base article: The Philosophy of SEPM Replication Setup

See "Setting up sites and replication" on page 187.

How to resolve data conflicts between sites during replication

If administrators change settings on the sites in a site farm, conflicts can occur.

Table 8-3 displays the ways that Symantec Endpoint Protection Manager handles the conflicts that arise.

	Table 8-3	How the management server resolves conflicts between sites

Conflict type	Example	Resolution
Two differences cannot exist together.	Administrators for site 1 and site 2 both configure an identical Firewall policy setting. On site 1, the setting is enabled. On site 2, the setting is disabled.	The management server retains only the most recently made change. For example, if you made a change on site 1 first, and site 2 second, then the site 2 change is retained.
The same variable is created for both sites.	Administrators on site 1 and site 2 both add a group with the same name.	The management server retains both changes, adding a tilde and the numeral 1 (~1) after the more recently made variable. For example, with two groups named as Sales, the most recently named Sales group becomes Sales ~1.
Data can merge without conflict.	The administrator for site 1 adds two Firewall policies and the administrator for site 2 adds five Firewall policies.	The management server merges the changes For example, the management server displays all seven Firewall policies on both sites.

See "How replication works" on page 191.

Replicating data on demand

Replication normally occurs according to the schedule that you set up when you added a replication partner during installation. The site with the smaller ID number initiates the scheduled replication. You might want replication to occur immediately.

If you use the Microsoft SQL Server database with more than one server, you can only initiate replication from the first server at that site.

See "Setting up sites and replication" on page 187.

Scheduling on-demand replication

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

2   Under **Servers**, expand **Replication Partners** and select the partner whose database you want to replicate immediately.

3   Under **Tasks**, click **Replicate Now**.

4   Click **Yes**.

5   Click **OK**.

Changing the automatic replication schedule

Replication normally occurs according to the schedule that you set up when you added a replication partner during the initial installation. The site with the smaller ID number initiates the scheduled replication. When a replication partner has been established, you can change the replication schedule. When you change the schedule on a replication partner, the schedule on both sides is the same after the next replication.

The time that it takes to replicate depends on the size of the database as well as network connection between the sites. First, test a replication cycle to see how long it takes. You should schedule your replication based on that time period, and make sure that the time when the management servers duplicate data does not overlap.

After the initial, full database replication, subsequent replications are fairly small, if you only replicate policies, clients, and groups, and not logs.

See "Setting up sites and replication" on page 187.

To change replication frequencies

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

2   Under **Servers**, click **Replication Partners**.

3   Under **Tasks**, click **Edit Replication Partner**.

4   In the **Edit Replication Partner** dialog box, specify the schedule for replication between the two partners by doing one of the following:

   ■ Check **Autoreplicate**.
     It causes frequent and automatic replication to occur between two sites. This option is the default setting. Therefore you cannot set up a custom schedule for replication.

     Note: The **Autoreplicate** option performs the replication process every two hours. Previous versions of the product automatically replicated every five minutes.

   ■ Uncheck **Autoreplicate**
     You can now set up a custom schedule for replication.

     ■ Select the hourly, daily, or weekly **Replication Frequency**.

■ Select the specific day during which you want replication to occur in the **Day of Week** list to set up a weekly schedule.

5   Click **OK**.

Specifying which data to replicate

You can choose to replicate or duplicate client packages, LiveUpdate content, and the logs between the local site and the remote site. The administrator at the remote site can then deploy the client package and LiveUpdate content.

If you decide to replicate client packages and LiveUpdate content, you may duplicate a large volume of data. The data in a client package might be as large as 5 GB. Both Symantec Endpoint Protection and Symantec Network Access Control 32- bit and 64-bit installation packages may require as much as 500 MB of disk space. If you plan to replicate logs, make sure that you have sufficient disk space for the additional logs on all the replication partner servers.

To specify which data to replicate

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

2   Under **Servers**, click **Replication Partners**.

3   Expand **Replication Partners** and select the replication partner with which you want to replicate client packages.

4   Under **Tasks**, click **Edit Replication Partner Properties**.

5   In the **Replication Partner Properties** dialog box, click **Replicate client packages and LiveUpdate content between local site and partner site**.

6   Click **OK**.

See "About client deployment methods" on page 131.

Deleting replication partners

When you remove a management server at a remote site, you need to manually delete it from all sites. Uninstalling the software from one management server console does not make the icon disappear from the **Servers** pane on other consoles.

To delete a replication partner

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

2   Under **Tasks**, click **Servers**.

3   Expand **Remote Sites** and select the site that you plan to delete.

4   Under **Tasks**, click **Delete Remote Site**.

5   Click **Yes**.

See "Re-adding a replication partner that you previously deleted" on page 197.

See "Setting up sites and replication" on page 187.

Re-adding a replication partner that you previously deleted

You can add a replication partner that was previously deleted as a partner. For example, you must delete replication partners before you migrate or upgrade to the latest version of the management server. Later you can add that replication partner back to make the databases consistent. However, some changes may collide. If you add a deleted partner, the management server to which you want to connect must have previously been a partner in the same site farm.

To re-add a replication partner that you previously deleted

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

2   Under **Servers**, select a site.

3   Under **Tasks**, click **Add Existing Replication Partner**.

4   In the **Add Specify Existing Replication Partner Wizard**, click **Next**.

5   In the **Remote Site Information** panel, type the IP address or host name and the port number of the management server that is the replication partner.

6   Type the administrator's user name and password for the remote management server, and then click **Next**.

7   In the **Schedule Replication** panel, specify the schedule for replication between the two partners by doing one of the following:

   ■   Check **Autoreplicate**.
       It causes frequent and automatic replication to occur between two sites.

   ■   To set up a custom schedule for replication, check **Autoreplicate**, and specify the schedule.

8   Click **Next**.

9   In the **Replication of Log Files and Client Packages** panel, check or uncheck the options depending on whether or not you want to replicate logs.

10   In the **Add Replication Partner** dialog box, do one of the following:

   ■   If the database has been restored on the replication partner site, click **Yes**.

You must restore the database on each replication partner site before you continue if you upgrade or restore a database.

■ Click **No** if the database has not been restored.
Then restore the database and restart this procedure.

11 Click **Next**.

12 Click **Finish**.

The replication partner is added under **Replication Partners** on the **Admin** page.

See "Turning off replication before upgrade" on page 168.

See "Turning on replication after upgrade" on page 169.

See "Deleting replication partners" on page 196.

See "Setting up sites and replication" on page 187.

Managing Symantec Endpoint Protection in Protection Center

This chapter includes the following topics:

- About Symantec Endpoint Protection and Protection Center

- About upgrading to Protection Center version 2

- About setting up Symantec Endpoint Protection in Protection Center

- About setting up multiple Symantec Endpoint Protection domains in Protection Center

- Configuring communication between Symantec Endpoint Protection Manager and Protection Center

About Symantec Endpoint Protection and Protection Center

Protection Center lets you manage Symantec Endpoint Protection together with other Symantec products in a single environment. Symantec Endpoint Protection is integrated with Protection Center by means of a series of Web services. These Web services provide communication between the Symantec Endpoint Protection Manager server and the Protection Center server.

You can perform the following tasks in Protection Center:

- Run the Symantec Endpoint Protection Manager console from Protection Center together with other Symantec product consoles.

The Symantec Endpoint Protection Manager console in Protection Center is almost identical to the standalone console. The main function options that appear to the left of the console window in the standalone version, however, appear at the top in Protection Center.

- Run the reports that contain data from Symantec Endpoint Protection and from other products, such as Symantec Messaging Gateway.
  The data feed Web services define the Symantec Endpoint Protection data that is written to the Protection Center database.

- Initiate the Protection Center workflows that include Symantec Endpoint Protection tasks. Protection Center provides the following Symantec Endpoint Protection workflows:

  - Quarantine Endpoint Workflow

  - Move Endpoint Workflow

  - Update Virus Definitions on Endpoint Workflow

  - Update Virus Definitions and Scan Endpoint Workflow

Other products may provide different tasks, or sets of integration points. For more information about how products can integrate with Protection Center, see the Protection Center documentation.

See "About upgrading to Protection Center version 2" on page 200.

See "About setting up Symantec Endpoint Protection in Protection Center" on page 201.

See "About setting up multiple Symantec Endpoint Protection domains in Protection Center" on page 202.

See "Configuring communication between Symantec Endpoint Protection Manager and Protection Center" on page 202.

For more information, see the Symantec Endpoint Protection and Symantec Protection Center Integration Guide.

About upgrading to Protection Center version 2

To upgrade to Protection Center version 2, you perform a new installation. You then add Symantec Endpoint Protection to Protection Center. The process of adding is similar to adding products in version 1.

See "About setting up Symantec Endpoint Protection in Protection Center" on page 201.

You set up user accounts in Protection Center to access integrated products differently, however. For more information, see the Protection Center documentation.

About setting up Symantec Endpoint Protection in Protection Center

You set up Symantec Endpoint Protection in Protection Center by performing the following tasks:

- Add the Symantec Endpoint Protection Manager server to Protection Center, and enable the server.
- Create Protection Center accounts to access Symantec Endpoint Protection and your other integrated products.
- Map the Protection Center accounts to the appropriate accounts in Symantec Endpoint Protection and your other integrated products.

For detailed information about how to add products and create accounts, see the Protection Center documentation.

You must set up multiple domains individually. If your Symantec Endpoint Protection Manager includes only the default domain, you do not need to specify any domain information in Protection Center.

See "About setting up multiple Symantec Endpoint Protection domains in Protection Center" on page 202.

Note: In Protection Center version 1, you can add Symantec Endpoint Protection by using a limited administrator account that has reporting rights. In version 2, you must use a system administrator or domain administrator account.

Protection Center can automatically discover the Symantec Endpoint Protection Manager servers in your network. This network discovery is enabled in Symantec Endpoint Protection Manager by default. If you disabled it, you can add Symantec Endpoint Protection Manager manually. For details about how to add a product manually, see the Protection Center documentation.

See "Configuring communication between Symantec Endpoint Protection Manager and Protection Center" on page 202.

About setting up multiple Symantec Endpoint Protection domains in Protection Center

To manage multiple Symantec Endpoint Protection domains in Protection Center, you must add each domain to Protection Center separately. You must specify the domain as part of the user name, in the form *<domain_name>\account_name*.

Note: Symantec Endpoint Protection domains are the equivalents of tenants in Protection Center. You also provide the domain name in the tenant field when you add a Symantec Endpoint Protection domain to Protection Center.

When you configure Symantec Endpoint Protection Manager, you configure ports for your entire system. You can use the default ports, or you can specify custom ports. When you add multiple domains in Protection Center, you must specify these ports for each domain that you add. The port numbers are the same, but Protection Center requires that you provide them for each domain.

Table 9-1 displays the terms Protection Center uses to refer to Symantec Endpoint Protection Manager ports.

Table 9-1　　　Port names

Protection Center port name	Symantec Endpoint Protection Manager port name
Data feed port	Web services port
Registration port	Web services port
Console port	Server port

See "About setting up Symantec Endpoint Protection in Protection Center" on page 201.

See "Configuring communication between Symantec Endpoint Protection Manager and Protection Center" on page 202.

Configuring communication between Symantec Endpoint Protection Manager and Protection Center

You can add a Symantec Endpoint Protection Manager to Protection Center by using the default communication settings that are installed when you install Symantec Endpoint Protection Manager.

In some cases, however, you may need to change some of these settings.

To configure communication between Symantec Endpoint Protection Manager and Protection Center

1   In the console, click **Admin > Servers > *Server name* > Edit Site Properties**.

2   On the **Web Services** tab, change any of the following settings:

Data Feeds	If you find that Protection Center data feeds consume too much of your network bandwidth, you can change these settings. **Note:** Data feeds are passed continually to Protection Center.
Workflow Size	Events trigger Protection Center workflows. Workflows are therefore less frequent than data feeds. You may still want to use these settings to refine how much the Protection Center workflows request Symantec Endpoint Protection data.
Network Discovery	If you disable Network Discovery, you must add Symantec Endpoint Protection Manager to Protection Center manually. See the Protection Center documentation for more information.
Authentication	Enable session-based authentication to let Symantec Technical Support or sales engineers write web service-based tools to help optimize your environment.

3   Click **OK**.

For more detailed information about these settings, see the context-sensitive help for the **Web Services** panel.

See "Enabling or disabling Symantec Endpoint Protection Manager web services" on page 720.

See "About setting up Symantec Endpoint Protection in Protection Center" on page 201.

Section **2**

Managing groups, clients, and administrators

Managing groups of client computers

This chapter includes the following topics:

Managing groups of clients

In Symantec Endpoint Protection Manager, groups function as containers for the endpoints that run the client software. These endpoints can be either computers, or users. You organize the clients that have similar security needs into groups to make it easier to manage network security.

Symantec Endpoint Protection Manager contains the following default groups:

- The **My Company** group is the top-level, or parent, group. It contains a flat tree of child groups.

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

Note: You cannot rename or delete the default groups.

Table 10-1   Group management actions

Task	Description
Add groups	See "How you can structure groups" on page 209.
	See "Adding a group" on page 210.
Import existing groups	If your organization already has an existing group structure, you can import the groups as organizational units.
	Note: You cannot manage imported organizational units in the same ways that you can manage the groups that you create in Symantec Endpoint Protection Manager.
	See "Importing existing groups and computers from an Active Directory or an LDAP server" on page 211.
Disable inheritance for subgroups	The subgroups inherit the same security settings from the parent group by default. You can disable inheritance.
	See "Disabling and enabling a group's inheritance" on page 218.
Create locations within groups	You can set up the clients to switch automatically to a different security policy if the physical location of the client changes.
	See "Managing locations for remote clients" on page 249.
	Some security settings are group-specific and some settings are location-specific. You can customize any settings that are location-specific.
	See "Configuring communication settings for a location" on page 259.
Assign clients to groups before you install the client software	See "Assigning clients to groups before you install the client software" on page 217.

Table 10-1   Group management actions *(continued)*

Task	Description
Manage security policies for groups	You can create security policies based on the needs of each group. You can then assign different policies to different groups or locations. See "Adding a policy" on page 296. See "Assigning a policy to a group" on page 300. See "Performing the tasks that are common to all policies" on page 290.
Perform basic group maintenance	You can move groups for easier management and move clients between groups. You can also block clients from being added to a particular group. See "Moving a client computer to another group" on page 219. See "Blocking client computers from being added to groups" on page 219.

How you can structure groups

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

Table 10-2   Criteria for creating groups

Criterion	Description
Function	You can create groups based on the types of computers to be managed, such as laptops, desktops, and servers. Alternatively, you can create multiple groups that are based on usage type. For example, you can create a remote group for the client computers that travel and a local group for the client computers that remain in the office.
Role	You can create groups for department roles, such sales, engineering, finance, and marketing.
Geography	You can create groups based on the offices, cities, states, regions, or countries where the computers are located.

Table 10-2   Criteria for creating groups *(continued)*

Criterion	Description
Combination	You can create groups based on a combination of criteria. For example, you can use the function and the role.
	You can add a parent group by role and add child subgroups by function, as in the following scenario:
	■ Sales, with subgroups of laptops, desktops, and servers.
	■ Engineering, with subgroups of laptops, desktops, and servers.

After you organize the client computers into group, you can apply the appropriate amount of security to that group.

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

If you have both Symantec Endpoint Protection clients and Symantec Network Access Control clients installed, keep the Symantec Endpoint Protection clients and Symantec Network Access Control clients in separate groups.

See the knowledge base article Best Practices for Creating Group Structure.

See

See

Adding a group

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

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

Note: You cannot add groups to the Default Group.

See

To add a group

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

2   Under **Clients**, select the group to which you want to add a new subgroup.

3   On the **Clients** tab, under **Tasks**, click **Add Group**.

4   In the **Add Group for** *group name* dialog box, type the group name and a description.

5   Click **OK**.

Importing existing groups and computers from an Active Directory or an LDAP server

If your company uses either Active Directory or an LDAP server to manage groups, you can import the group structure into Symantec Endpoint Protection Manager. You can then manage the groups and computers from the management console.

Table 10-3 lists the tasks you should perform to import the group structure before you can manage them.

Table 10-3   Importing existing groups and computers

Step	Task	Description
Step 1	Connect Symantec Endpoint Protection Manager to your company's directory server	You can connect Symantec Endpoint Protection Manager to either Active Directory or an LDAP-compatible server. When you add the server, you should enable synchronization.
		See "About importing organizational units from the directory server" on page 212.
		See "Connecting Symantec Endpoint Protection Manager to a directory server" on page 213.
		See "Connecting to a directory server on a replicated site" on page 215.
Step 2	Import either entire organizational units or specific computer accounts or user accounts	You can either import the existing group structure, or import individual computer accounts or user accounts into the Symantec Endpoint Protection Manager groups that you create.
		See "Importing organizational units from a directory server" on page 215.
		If you want to use the group structure of Symantec Endpoint Protection Manager and not the directory server, import individual accounts.
		See "Searching for and importing specific accounts from a directory server" on page 216.

	Table 10-3	Importing existing groups and computers *(continued)*

Step	Task	Description
Step 3	Either keep imported computer or user accounts in their own group or copy imported accounts to existing groups	After you import organizational units, you can do either of the following actions:
		■ Keep the imported organizational units or accounts in their own groups. After you import organizational units or individual accounts, you assign policies to the organizational unit or group.
		■ Copy the imported accounts to existing Symantec Endpoint Protection Manager groups. The copied accounts follow the policy of the Symantec Endpoint Protection Manager group and not the imported organizational unit.
		See "Adding a group" on page 210.
		See "Assigning a policy to a group" on page 300.
		See "The types of security policies" on page 293.
Step 4	Change the authentication method for administrator accounts (optional)	For the administrator accounts that you added in Symantec Endpoint Protection Manager, change the authentication method to use directory server authentication instead of the default Symantec Endpoint Protection Manager authentication. You can use the administrator accounts to authenticate the accounts that you imported. When an administrator logs on to Symantec Endpoint Protection Manager, the management server retrieves the user name from the database and the password from the directory server.
		See "Changing the authentication method for administrator accounts" on page 275.
		See "Best practices for testing whether a directory server authenticates an administrator account" on page 278.

About importing organizational units from the directory server

Microsoft Active Directory and LDAP servers use organizational units to manage accounts for computers and users. You can import an organizational unit and its account data into Symantec Endpoint Protection Manager, and manage the account data in the management console. Because Symantec Endpoint Protection Manager treats the organizational unit as a group, you can then assign a security policy to the organizational unit group.

You can also move accounts from the organizational units into a Symantec Endpoint Protection Manager group by copying the accounts. The same account then exists in both the Symantec Endpoint Protection Manager group and the organizational unit. Because the priority of the Symantec Endpoint Protection

Manager group is higher than the organizational unit, the copied accounts adopt
the policy of the Symantec Endpoint Protection Manager group.

If you delete an account from the directory server that you copied to a Symantec
Endpoint Protection Manager group, the account name still remains in the
Symantec Endpoint Protection Manager group. You must remove the account
from the management server manually.

If you need to modify the account data in the organizational unit, you perform
this task on the directory server, and not in Symantec Endpoint Protection
Manager. For example, you can delete an organizational unit from the management
server, which does not permanently delete the organizational unit in the directory
server. You must synchronize Symantec Endpoint Protection Manager with the
Active Directory server so that these changes get automatically updated in
Symantec Endpoint Protection Manager. You enable synchronization when you
set up the connection to the directory server.

Note: Synchronization is only possible for Active Directory Servers. Symantec
Endpoint Protection does not support synchronization with LDAP servers.

You can also import selected users to a Symantec Endpoint Protection Manager
group rather than importing the entire organizational unit.

See "Connecting Symantec Endpoint Protection Manager to a directory server"
on page 213.

See "Importing existing groups and computers from an Active Directory or an
LDAP server" on page 211.

See "Importing organizational units from a directory server" on page 215.

See "Searching for and importing specific accounts from a directory server"
on page 216.

Connecting Symantec Endpoint Protection Manager to a directory server

You must first connect Symantec Endpoint Protection Manager to your company's
directory server before you can import the organizational units that contain
computer accounts or user accounts.

You cannot modify the accounts in organizational units in the management server,
only in the directory server. However, you can synchronize the account data
between an Active Directory server and the management server. Any changes
you make in the Active Directory server are automatically updated in Symantec
Endpoint Protection Manager. Any changes that you make on the Active Directory

server do not appear immediately in the organizational unit that was imported into the management server. The latency period depends on the synchronization frequency. You enable synchronization and set the synchronization frequency when you configure the connection.

If you delete a directory server connection from Symantec Endpoint Protection Manager, you must first delete any organizational units that you imported that are associated with that connection. Then you can synchronize data between the servers.

Note: Synchronization is only possible for Active Directory Servers. Symantec Endpoint Protection does not support synchronization with LDAP servers.

To connect Symantec Endpoint Protection Manager to a directory server

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

2   Under **Servers** and **Local Site**, select the management server.

3   Under **Tasks**, click **Edit the server properties**.

4   In the **Server Properties** dialog box, on the **Directory Servers** tab, click **Add**.

5   In the **Add Directory Server** dialog box, type a name for the directory server.

6   Check **Active Directory** or **LDAP** and type the IP address, host name, or domain name.

    If you add an LDAP server, change the port number of the LDAP server if it should be different than the default value.

7   If you want an encrypted connection, check **Use Secure Connection**.

8   Click **OK**.

9   On the **Directory Servers** tab, check **Synchronize with Directory Servers** and under **Schedule**, set up the synchronization schedule.

10 Click **OK**.

See "Importing organizational units from a directory server" on page 215.

See "Searching for and importing specific accounts from a directory server" on page 216.

See "Importing existing groups and computers from an Active Directory or an LDAP server" on page 211.

Connecting to a directory server on a replicated site

If a site uses a replicated Active Directory or LDAP server, you can connect Symantec Endpoint Protection Manager to both the primary directory server and the replicated server. If the primary directory server gets disconnected, the management server stays connected to the replicated directory server.

Symantec Endpoint Protection Manager can then authenticate administrator accounts and synchronize organizational units on all the Active Directory servers of the local site and the replicated sites.

See "Setting up sites and replication" on page 187.

Note: Synchronization is only possible for Active Directory Servers. Symantec Endpoint Protection does not support synchronization with LDAP servers.

To connect to a directory server on a replicated site

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

2   Under **Servers**, select the management server.

3   Under **Tasks**, click **Edit the server properties**.

4   In the **Server Properties** dialog box, on the **Directory Servers** tab, click **Add**.

5   In the **Add Directory Server** dialog box, on the **Replication Servers** tab, click **Add**.

6   In the **Add Replication Server** dialog box, type the IP address, host name, or domain name for the directory server, and then click **OK**.

7   Click **OK**.

8   Click **OK**.

See "Connecting Symantec Endpoint Protection Manager to a directory server" on page 213.

Importing organizational units from a directory server

When you import computer accounts or user accounts from an Active Directory or LDAP server, you import these accounts as organizational units. You can then apply a security policy to the organizational unit. You can also copy these accounts to an existing Symantec Endpoint Protection Manager group.

You can import the organizational unit as a subgroup of either the **My Company** group or a group you create, but not the **Default Group**. You cannot create groups as a subgroup of an organizational unit. You cannot place an organizational unit in more than one Symantec Endpoint Protection Manager group.

If you do not want to import all computer accounts or user accounts within a group, then you can select and import specific accounts.

See "Searching for and importing specific accounts from a directory server" on page 216.

Note: Before you import organizational units into Symantec Endpoint Protection Manager, you must convert some of the special characters that precede a computer name or user name. You perform this task in the directory server. If you do not convert special characters, the management server does not import these accounts.

You must convert the following special characters:

- A space or a hash character (#) that occurs at the beginning of an entry.
- A space character that occurs at the end of an entry.
- A comma (,), plus sign (+), double quotation mark ("), less than or greater than symbols (< or >), equals sign (=), semi-colon (;), backslash (\).

To allow a name that includes these characters to be imported, you must precede each character with a backslash character (\).

To import organizational units from a directory server

1   Connect Symantec Endpoint Protection Manager to a directory server.

    See "Connecting Symantec Endpoint Protection Manager to a directory server" on page 213.

2   In the console, click **Clients**, and under **Clients**, select the group to which you want to add the organizational unit.

3   Under **Tasks**, click **Import Organizational Unit or Container**.

4   In the **Domain** drop-down list, choose the directory server name you created in step 1.

5   Select either the domain or a subgroup.

6   Click **OK**.

See "Importing existing groups and computers from an Active Directory or an LDAP server" on page 211.

See "About importing organizational units from the directory server" on page 212.

Searching for and importing specific accounts from a directory server

You can import specific computer accounts or user accounts rather than an entire group structure from a directory server into Symantec Endpoint Protection

Manager groups. You should import specific accounts if you want to apply different security policies for the accounts in an organizational unit.

For example, you might want to maintain remote computers in one group. You would create a group for remote computers and assign a group policy that is tailored for remote computers in that group. You can then search for and import computers from the organizational unit directly to the remote group.

If you do not want to import specific accounts, then you can import all accounts within an organizational unit.

To search for and import specific accounts from a directory server

1   Connect to a directory server.

    See "Connecting Symantec Endpoint Protection Manager to a directory server" on page 213.

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

3   On the **Clients** tab, under **Tasks**, click **Import Active Directory or LDAP Users**.

4   In the **Import Active Directory or LDAP Users** dialog box, select the server name in the **Directory Server** drop-down list.

    The user name and password of the server automatically appears.

    If **Only show users that are not added in any group** is checked, only those accounts appear that have not already been added.

5   Click **List Users**.

    In the **LDAP Filter** field, you can also type an LDAP query to locate the names of accounts that you want to import.

    For more information, click **Help**.

6   To select specific accounts, click **Add**, or click **Add All**.

7   Click **Close**.

See "Importing organizational units from a directory server" on page 215.

Assigning clients to groups before you install the client software

You can assign your clients to their groups before you install the client software. If you perform this task first, you can assign security policies to the client separately from the installation. In this case, the client does not receive the security

policies from the group that is specified in the client installation package. Instead, the client is assigned to the group that you specified before installation.

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

See "Switching a client between user mode and computer mode" on page 234.

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

See "Blocking client computers from being added to groups" on page 219.

To assign clients to groups before you install the client software

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

2   On the **Clients** page, under **Clients**, locate the group to which you want to add a client.

3   On the **Clients** tab, under **Tasks**, do one of the following actions:

    ■   For user mode, click **Add User Account**. Enter the user name. If the user is part of a Windows Domain, type the domain name. If the user is part of a workgroup, click **Log on local computer**.

    ■   For computer mode, click **Add Computer Account**. Type the computer name and then type the Windows Domain name or type `Workgroup`.

4   Click **OK**.

Disabling and enabling a group's inheritance

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

See "Managing groups of clients" on page 207.

To disable or enable a group's inheritance

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

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

You can select any group except the top-level group, My Company.

3 In the *group name* pane, on the **Policies** tab, do one of the following tasks:

■ To disable inheritance, uncheck **Inherit policies and settings from parent group "***group name***"**.

■ To enable inheritance, check **Inherit policies and settings from parent group "***group name***"**, and then click **Yes** when asked to proceed.

Blocking client computers from being added to groups

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

See "Managing client installation packages" on page 150.

You can block a client if you do not want clients to be added automatically to a specific group when they connect to the network. You can block a new client from being added to the group to which they were assigned in the client installation package. In this case, the client gets added to the default group. You can manually move a computer to a blocked group.

To block client computers from being added to groups

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

2 Under **Clients**, right-click a group, and click **Properties**.

3 On the **Details** tab, under **Tasks**, click **Edit Group Properties**.

4 In the **Group Properties for *group name*** dialog box, click **Block New Clients**.

5 Click **OK**.

See "Moving a client computer to another group" on page 219.

Moving a client computer to another group

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

To move client from multiple groups into a single group, you can redeploy the client installation package.

See "Restoring client-server communications by using a client installation package" on page 701.

To move a client computer to another group

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

2   On the **Clients** page, on the **Computers** tab, select a group

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

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

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

5   Click **OK**.

See "Managing groups of clients" on page 207.

Managing clients

This chapter includes the following topics:

Managing client computers

Table 11-1 lists the tasks you should perform with the computers after you install the client software.

Table 11-1   Tasks to manage client computers

Task	Description
Check that the client software is installed on your computers	■ You can display the computers in each group that do not have the client software installed yet. See "Displaying which clients do not have the client software installed" on page 227. ■ You can configure a client computer to detect that other devices do not have the client software installed. Some of these devices might be unprotected computers. You can then install the client software on these computers. See "Configuring a client to detect unmanaged devices" on page 236. ■ You can add a client to a group and install the client software later. See "About client deployment methods" on page 131.
Check whether the client is connected to the management server	You can check the client status icons in the management console and in the client. The status icon shows whether the client and the server communicate. See "How to determine whether the client is connected in the console" on page 224. See "How to determine whether the client is connected and protected" on page 697. A computer may have the client software installed, but is an unmanaged client. You cannot manage an unmanaged client. Instead, you can convert the unmanaged client to a managed client. See "Why do I need to replace the client-server communications file on the client computer?" on page 698.
Configure the connection between the client and the server	After you install the client software client computers automatically connect to the management server at the next heartbeat. You can change how the server communicates with the client computer. See "Managing the client-server connection" on page 696. You can troubleshoot any connection issues. See "Troubleshooting communication problems between the management server and the console or the database" on page 766.

Table 11-1   Tasks to manage client computers *(continued)*

Task	Description
Check that client computers have the right level of protection	■ You can view the status of each protection technology on your client computers. See "Viewing the protection status of clients and client computers" on page 226. See "How to determine whether the client is connected in the console" on page 224. ■ You can run reports or view logs to see whether you need to increase protection or improve performance. For example, the scans may cause false positives. You can also identify the client computers that need protection. See "Monitoring endpoint protection" on page 603. ■ You can modify protection based on specific attributes of the client software or the client computers. See "Searching for information about client computers" on page 228.
Adjust the protection on client computers	If you decide that clients do not have the right level of protection, you can adjust the protection settings. ■ You can increase or decrease each type of protection based on the results in the reports and logs. See "The types of security policies" on page 293. See "About the types of threat protection that Symantec Endpoint Protection provides" on page 46. ■ You can temporarily disable protection on the client computers if you need to diagnose a problem or improve performance. See "About enabling and disabling protection when you need to troubleshoot problems" on page 229. See "Running commands on the client computer from the console" on page 233. ■ You can require a password on the client. See "Password-protecting the client" on page 245.
Move endpoints from one group to another to modify protection (optional)	To change a client computer's level of protection, you can move it to a group that provides more protection or less protection. See "Moving a client computer to another group" on page 219. When you deploy a client installation package, you specify which group the client goes in. You can move the client to a different group. But if the client gets deleted or disconnected and then gets added again and reconnected, the client returns to the original group. To keep the client with the group it was last moved to, configure the reconnection preferences. You configure these settings in the **Communications Settings** dialog box on the **Clients > Policies** tab.

Table 11-1 Tasks to manage client computers *(continued)*

Task	Description
Let users control computer protection (optional)	You can specify the kind of control that users have over the protection on client computers. ■ For Virus and Spyware Protection and Proactive Threat Protection, you can lock or unlock a check box to specify whether users can change individual settings. See "Locking and unlocking Virus and Spyware policy settings" on page 299. ■ For the Firewall policy and the IPS policy and for some client user interface settings, you can change the user control level more generally. See "Changing the user control level" on page 239. ■ If users need full control of the client, you can install an unmanaged client. See "Why do I need to replace the client-server communications file on the client computer?" on page 698.
Remove the client software from computers (optional)	If a computer is no longer used and you want to use the license for a different computer, you can delete the client from the database after a certain number of days. By deleting a client, you also save space in the database. See "Uninstalling the Windows client" on page 149. See "Uninstalling the Mac client" on page 149.

See "Managing protection on client computers" on page 60.

How to determine whether the client is connected in the console

In Symantec Endpoint Protection Manager, you can use the client status icons to check whether the client and the server communicate.

Table 11-2 Client status icons in the management console

Icon	Description
	This icon indicates the following status: The client software installation failed.
	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode.

Table 11-2   Client status icons in the management console *(continued)*

Icon	Description
	This icon indicates the following status: ■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client may have been added from the console, and may not have any Symantec client software installed.
	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client is an unmanaged detector.
	This icon indicates the following status: ■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in computer mode. ■ The client is an unmanaged detector.
	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager. ■ The client is in user mode.
	This icon indicates the following status: ■ The client cannot communicate with Symantec Endpoint Protection Manager. ■ The client is in user mode. ■ The client may have been added from the console, and may not have any Symantec client software installed.
	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in computer mode.

Table 11-2 Client status icons in the management console *(continued)*

Icon	Description
⊕	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in computer mode. ■ The client is an unmanaged detector.
🛡	This icon indicates the following status: ■ The client can communicate with Symantec Endpoint Protection Manager at another site. ■ The client is in user mode.

See "Viewing the protection status of clients and client computers" on page 226.

You can also look on the client to see whether or not it is connected to the management server.

See "How to determine whether the client is connected and protected" on page 697.

Viewing the protection status of clients and client computers

You can view information about the real-time operational and protection status of the clients and the computers in your network.

You can view:

■ A list of managed client computers that do not have the client installed.
  You can view the computer name, the domain name, and the name of the user who is logged on.

■ If the client is a virtual machine in a VMware infrastructure that uses a Security Virtual Appliance, the Security Virtual Appliance that the client is associated with.

■ Which protections are enabled and disabled.

■ Which client computers have the latest policies and definitions.

■ The group's policy serial number and the client's version number.

■ The information about the client computer's network components, such as the MAC address of the network card that the computer uses.

- The system information about the client computer, such as the amount of available disk space and the operating system version number.

After you know the status of a particular client, you can resolve any security issues on the client computers. You can resolve many issues by running commands on groups. For example, you can update content, or enable Auto-Protect.

Note: If you manage legacy clients, some newer protection technologies may be listed as **not reporting**. This behavior is expected. It does not mean that you need to take action on these clients.

See "How to determine whether the client is connected in the console" on page 224.

See "Running commands on the client computer from the console" on page 233.

See "Displaying which clients do not have the client software installed" on page 227.

To view the protection status of client computers

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

2   On the Clients page, under **Clients**, locate the group that contains the clients that you want information about.

3   On the **Clients** tab, click the **View** drop-down list. Then, select a category.

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

Displaying which clients do not have the client software installed

You can display which clients in a group appear on the **Clients** tab, based on the following criteria:

- Client software is installed.

- Clients run either Windows or Mac computers

- Clients are in computer mode or user mode.

- Clients are non-persistent and offline in Virtual desktop infrastructures.

You can also configure how many clients appear on each page to make the list easier to manage.

Note: The Symantec Endpoint Protection Manager retains the Client View Filter setting and stores it with the login name of the individual administrator or limited administrator. If an administrator sets a filter condition, that condition is retained for that administrator. Different administrators see only the filters that they have set themselves.

See "Viewing the protection status of clients and client computers" on page 226.

See "How to determine whether the client is connected in the console" on page 224.

To display which clients do not have the client software installed

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

2   In the **Clients** pane, choose the group you want to search on.

3   On the **Clients** tab, under **Tasks**, click **Set display filter**.

4   In the **Set Display Filter** dialog box, check the criteria for which you want to filter and display the client computers.

5   To shorten the list, click **Results per page** and enter the number of results to show on each page.

    Valid values range from 1 to 1000.

6   Click **OK**.

Searching for information about client computers

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

See "Viewing the protection status of clients and client computers" on page 226.

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

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

See "Collecting user information" on page 244.

To search for information about client computers

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

2   On the **Clients** tab, under **View Clients**, choose the group you want to search.

3   Under **Tasks**, click **Search clients**.

4   In the **Search clients** dialog box, in the Find drop-down list, click either **Computers** or **Users**.

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

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

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

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

    You can use standard Boolean operators in your search criteria.

9   In the **Value** cell, type the search string.

10 Click **Search**.

    You can export the results into a text file.

11 Click **Close**.

About enabling and disabling protection when you need to troubleshoot problems

In general, you always want to keep the protection technologies enabled on a client computer.

You might need to temporarily disable either all the protection technologies or individual protection technologies if you have a problem with the client computer. For example, if an application does not run or does not run correctly, you might want to disable Network Threat Protection. If you still have the problem after you disable all protection technologies, completely uninstall the client. If the problem persists, you know that the problem is not due to Symantec Endpoint Protection.

Warning: Be sure to enable again any of the protections when you have completed your troubleshooting task to ensure that the computer remains protected.

Table 11-3 describes the reasons why you might want to disable each protection technology.

Table 11-3   Purpose for disabling a protection technology

Protection technology	Purpose for disabling the protection technology
Virus and Spyware Protection	If you disable this protection, you disable Auto-Protect only. The scheduled or startup scans still run if you or the user has configured them to do so. You might enable or disable Auto-Protect for the following reasons: ■ Auto-Protect might block you from opening a document. For example, if you open a Microsoft Word that has a macro, Auto-Protect may not let you open it. If you know the document is safe, you can disable Auto-Protect. ■ Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. For example, you might get a warning when you install new computer applications. If you plan to install more applications and you want to avoid the warning, you can temporarily disable Auto-Protect. ■ Auto-Protect may interfere with Windows driver replacement. ■ Auto-Protect might slow down the client computer. **Note:** If you disable Auto-Protect, you also disable Download Insight, even if Download Insight is enabled. SONAR also cannot detect heuristic threats. SONAR detection of host file and system changes continues to function. See "Running commands on the client computer from the console" on page 233. If Auto-Protect causes a problem with an application, it is better to create an exception than to permanently disable the protection. See "Creating exceptions for Symantec Endpoint Protection" on page 530.
Proactive Threat Protection	You might want to disable Proactive Threat Protection for the following reasons: ■ You see too many warnings about the threats that you know are not threats. ■ Proactive Threat Protection might slow down the client computer. See "Adjusting SONAR settings on your client computers" on page 402.

| | Table 11-3 | Purpose for disabling a protection technology *(continued)* |

Protection technology	Purpose for disabling the protection technology
Network Threat Protection	You might want to disable Network Threat Protection for the following reasons: ■ You install an application that might cause the firewall to block it. ■ The firewall or the Intrusion Prevention System causes network connectivity-related issues. ■ The firewall might slow down the client computer. ■ You cannot open an application. If you are not sure that Network Threat Protection causes the problem, you might need to disable all the protection technologies. You can configure Network Threat Protection so that users cannot enable or disable it. You can also set the following limits for when and how long the protection is disabled: ■ Whether the client allows either all traffic or all outbound traffic only. ■ The length of time the protection is disabled. ■ How many times you can disable protection before you restart the client. See "Enabling or disabling network intrusion prevention or browser intrusion prevention" on page 467. See "Configuring user interface settings" on page 242.
Tamper Protection	Typically, you should keep Tamper Protection enabled. You might want to disable Tamper Protection temporarily if you get an extensive number of false positive detections. For example, some third-party applications might make the changes that inadvertently try to modify Symantec settings or processes. If you are sure that an application is safe, you can create a Tamper Protection exception for the application. See "Changing Tamper Protection settings" on page 412.

About commands that you can run on client computers

You can run commands remotely on individual clients or an entire group from the console.

You can enable and disable protection to troubleshoot problems on the client computer.

See "About enabling and disabling protection when you need to troubleshoot problems" on page 229.

Table 11-4   Commands that you can run on client computers

Commands	Description
Scan	Runs on-demand scan on the client computers. If you run a scan command, and select a **Custom** scan, the scan uses the command scan settings that you configured on the **Administrator-defined Scans** page. The command uses the settings that are in the Virus and Spyware Protection policy that is applied to the selected client computers. See "Running on-demand scans on client computers" on page 344.
Update Content	Updates content on clients by initiating a LiveUpdate session on the client computers. The clients receive the latest content from Symantec LiveUpdate. See "Configuring the LiveUpdate download schedule for Symantec Endpoint Protection Manager" on page 563.
Update Content and Scan	Updates content by initiating a LiveUpdate session and runs an on-demand scan on client computers.
Restart Client Computers	Restarts the client computers. If users are logged on to the client, they are warned based on the restart options that the administrator has configured for that client. You can configure client restart options on the **General Settings** tab. **Note:** Some restart options apply differently to Mac clients and to Windows clients. See "Restarting client computers" on page 145. **Note:** You can ensure that a client does not restart. You can add a registry key on the client that keeps it from restarting even if an administrator issues a restart command. See "Ensuring that a client does not restart" on page 234.

Table 11-4   Commands that you can run on client computers *(continued)*

Commands	Description
Enable Auto-Protect	Enables Auto-Protect for the file system on the client computers.
	By default, Auto-Protect for the file system is enabled. You might need to enable Auto-Protect from the console if you have allowed users to change the setting or if you disable Auto-Protect. You can lock the setting so that users on client computers cannot disable Auto-Protect.
	See "Customizing Auto-Protect for Windows clients" on page 378.
	See "Customizing Auto-Protect for Mac clients" on page 379.
	If you want to enable or disable Auto-Protect for email, you must include the setting in the Virus and Spyware Protection policy.
Enable Network Threat Protection and **Disable Network Threat Protection**	Enables or disables the firewall and enables intrusion prevention on the client computers.
	Note: Mac client computers do not process this command.
	See "Managing firewall protection" on page 413.
Enable Download Insight and **Disable Download Insight**	Enables or disables Download Insight on the client computers.
	Note: Mac client computers do not process this command.
	See "Managing Download Insight detections" on page 351.

See "Running commands on the client computer from the console" on page 233.

See "Running commands from the computer status log" on page 630.

You can configure a limited administrator to have rights to some or none of these commands.

See "Configuring the access rights for a limited administrator" on page 274.

Running commands on the client computer from the console

On managed clients, the commands that you run override the commands that the user runs. The order in which commands and actions are processed on the client computer differs from command to command. Regardless of where the command is initiated, commands and actions are processed in the same way.

You can also run these commands on clients from the **Computer Status** log.

See "Running commands from the computer status log" on page 630.

See "About commands that you can run on client computers" on page 231.

To run commands on the client computer from the console

1   In the console, click **Clients**, and then under **Computers**, select the group that includes computers for which you want to run a command.

2   Do one of the following actions:

■   In the left pane, under **Computers**, right-click the group for which you want to run the command.

■   In the right pane, on the **Clients** tab, select and right-click the computers or users for which you want to run the command.

3   Click one of the following commands:

■   **Run Command on Group > *command***

■   **Run Command on Clients > *command***

4   In the message that appears, click **OK**.

Ensuring that a client does not restart

You can use the following procedure to ensure that any Symantec Endpoint Protection client computer does not restart. For example, you may want to set this value on the servers that run the Symantec Endpoint Protection client. Setting this registry key ensures that the server does not restart if an administrator issues a Restart computer command on its group from the console.

To ensure that a client does not restart

1   On the client computer, open the registry editor.

2   Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC.

3   Add the following line to the registry:

```
DisableRebootCommand   REG_DWORD   1
```

Switching a client between user mode and computer mode

You add clients to be in either user mode or computer mode, based on how you want to apply policies to the clients in groups. After a user or a computer is added to a group, it assumes the policies that were assigned to the group.

When you add a client, it defaults to computer mode, which takes precedence over user mode. Symantec recommends that you use computer mode.

Mode	Description
Computer mode	The client computer gets the policies from the group of which the computer is a member. The client protects the computer with the same policies, regardless of which user is logged on to the computer. The policy follows the group that the computer is in. Computer mode is the default setting. Many organizations configure a majority of clients in computer mode. Based on your network environment, you might want to configure a few clients with special requirements as users.
	You cannot switch from user mode to computer mode if the computer name is already in another group. Switching to computer mode deletes the user name of the client from the group and adds the computer name of the client into the group.
	Clients that you add in computer mode can be enabled as unmanaged detectors, and used to detect unauthorized devices.
	See "Configuring a client to detect unmanaged devices" on page 236.
User mode	The client computer gets the policies from the group of which the user is a member. The policies change, depending on which user is logged on to the client. The policy follows the user.
	You cannot switch from computer mode to user mode if the user's logon name and the computer name are already contained in any group. Switching to user mode deletes the computer name of the client from the group. It then adds the user name of the client into the group.

When you deploy a client installation package, you specify which group the client goes in. You can later specify the client to be in user mode or computer mode. If the client later gets deleted or disconnected and then gets added again and reconnected, the client returns to the original group. However, you can configure the client to stay with the group it was last moved to in user mode or computer mode. For example, a new user might log on to a client that is configured in user mode. The client then stays in the group that the previous user was in.

You configure these settings by clicking **Clients** > **Policies**, and then **Communications Settings**.

To switch a client between user mode and computer mode

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

2   On the **Clients** page, under **Clients**, select the group that contains the user or computer.

3   On the **Clients** tab, right-click the computer or the user name in the table, and then select either **Switch to Computer Mode** or **Switch to User Mode**.

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

See "Assigning clients to groups before you install the client software" on page 217.

Configuring a client to detect unmanaged devices

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

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

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

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

■   Enable Network Threat Protection.
    See "Running commands on the client computer from the console" on page 233.

■   Switch the client to computer mode.
    See "Switching a client between user mode and computer mode" on page 234.

- Install the client on a computer that runs all the time.

- Enable Symantec Endpoint Protection clients as unmanaged detectors.
  A Symantec Network Access Control client cannot be an unmanaged detector.

To configure a client to detect unauthorized devices

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

2   Under **Clients**, select the group that contains the client that you want to
     enable as an unmanaged detector.

3   On the **Clients** tab, right-click the client that you want to enable as an
     unmanaged detector, and then click **Enable as Unmanaged Detector**.

4   To specify one or more devices to exclude from detection by the unmanaged
     detector, click **Configure Unmanaged Detector**.

5   In the **Unmanaged Detector Exceptions for *client name*** dialog box, click
     Add.

6   In the **Add Unmanaged Detector Exception** dialog box, click one of the
     following options:

     - **Exclude detection of an IP address range**, and then enter the IP address
       range for several devices.

     - **Exclude detection of a MAC address**, and then enter the device's MAC
       address.

7   Click **OK**.

8   Click **OK**.

To display the list of unauthorized devices that the client detects

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

2   On the **Home** page, in the **Security Status** section, click **More Details**.

3   In the **Security Status Details** dialog box, scroll to the **Unknown Device
     Failures** table.

4   Close the dialog box.

About access to the client interface

You can determine the level of interaction that you want users to have on the
Symantec Endpoint Protection client. Choose which features are available for
users to configure. For example, you can control the number of notifications that
appear and limit users' ability to create firewall rules and virus and spyware scans.
You can also give users full access to the user interface.

The features that users can customize for the user interface are called managed settings. The user does not have access to all the client features, such as password protection.

To determine the level of user interaction, you can customize the user interface in the following ways:

■ For virus and spyware settings, you can lock or unlock the settings.
See "Locking and unlocking Virus and Spyware policy settings" on page 299.

■ For firewall settings, intrusion prevention settings, and for some client user interface settings, you can set the user control level and configure the associated settings.
See "Configuring user interface settings" on page 242.
See "Changing the user control level" on page 239.
See "Configuring firewall settings for mixed control" on page 421.

■ You can password-protect the client.
See "Password-protecting the client" on page 245.

About mixed control

For clients in mixed control, you can determine which managed options you want users to configure or not. Managed options include settings in a Firewall policy, an Intrusion Prevention policy, and the client user interface settings.

For each option, you can assign it to server control or you can assign it to client control. In client control, only the user can enable or disable the setting. In server control, only you can enable or disable the setting. Client control is the default user control level. If you assign an option to server control, you then configure the setting in the corresponding page or dialog box in the Symantec Endpoint Protection Manager console. For example, you can enable the firewall settings in the Firewall policy. You can configure the logs in the Client Log Settings dialog box on the Policies tab of the Clients page.

You can configure the following types of settings:

■ User interface settings
See "Enabling or disabling network intrusion prevention or browser intrusion prevention" on page 467.

■ General Network Threat Protection settings
See "Configuring firewall settings for mixed control" on page 421.

■ Firewall policy settings
See "About the Symantec Endpoint Protection firewall" on page 415.

■ Intrusion Prevention policy settings

Changing the user control level

You can determine whether or not certain protection technology features and client user interface settings are available for users to configure on the Symantec Endpoint Protection client. To determine which settings are available, you specify the user control level. The user control level determines whether the client can be completely invisible, display a partial set of features, or display a full user interface.

In Symantec Endpoint Protection releases prior to 12.1, a change from client control to server control causes all settings, regardless of their lock status, to revert to their server control default values the next time policies are distributed to clients. In 12.1, locks are in effect in all control modes. Unlocked settings behave as follows in server control and client control modes:

- In Server Control, changes can be made to unlocked settings, but they are overwritten when the next policy is applied.

- In Client Control, client-modified settings take precedence over server settings. They are not overwritten when the new policy is applied, unless the setting has been locked in the new policy.

Note: The Symantec Network Access Control client only runs in server control. Users cannot configure any user interface settings.

Table 11-5	User control levels
User control level	**Description**
Server control	Gives the users the least control over the client. Server control locks the managed settings so that users cannot configure them. Server control has the following characteristics: ■ Users cannot configure or enable firewall rules, application-specific settings, firewall settings, intrusion prevention settings, or Network Threat Protection and Client Management logs. You configure all the firewall rules and security settings for the client in Symantec Endpoint Protection Manager. ■ Users can view logs, the client's traffic history, and the list of applications that the client runs. ■ You can configure certain user interface settings and firewall notifications to appear or not appear on the client. For example, you can hide the client user interface. The settings that you set to server control either appear dimmed or are not visible in the client user interface. When you create a new location, the location is automatically set to server control.
Client control	Gives the users the most control over the client. Client control unlocks the managed settings so that users can configure them. Client control has the following characteristics: ■ Users can configure or enable firewall rules, application-specific settings, firewall notifications, firewall settings, intrusion prevention settings, and client user interface settings. ■ The client ignores the firewall rules that you configure for the client. You can give client control to the client computers that employees use in a remote location or a home location.

Table 11-5   User control levels *(continued)*

User control level	Description
Mixed control	Gives the user a mixture of control over the client. Mixed control has the following characteristics: ■ Users can configure the firewall rules and application-specific settings. ■ You can configure the firewall rules, which may or may not override the rules that users configure. The position of the server rules in the Rules list of the firewall policy determines whether server rules override client rules. ■ You can specify certain settings to be available or not available on the client for users to enable and configure. These settings include the Network Threat Protection logs, Client Management logs, firewall settings, intrusion prevention settings, and some user interface settings. ■ You can configure Virus and Spyware Protection settings to override the setting on the client, even if the setting is unlocked. For example, if you unlock the Auto-Protect feature and the user disables it, you can enable Auto-Protect. The settings that you set to client control are available to the user. The settings that you set to server control either appear dimmed or are not visible in the client user interface. See "About mixed control" on page 238.

Some managed settings have dependencies. For example, users may have permission to configure firewall rules, but cannot access the client user interface. Because users do not have access to the Configure Firewall Rules dialog box, they cannot create rules.

You can set a different user control level for each location.

Note: Clients that run in client control or mixed control switch to server control when the server applies a Quarantine policy.

To change the user control level

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

2   Under View Clients, select the group whose location you want to modify.

3   Click the **Policies** tab.

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

5   To the right of Client User Interface Control Settings, click **Tasks > Edit Settings**.

6   In the Client User Interface Control Settings dialog box, do one of the following options:

■ Click **Server control**, and then click **Customize**.
Configure any of the settings, and then click **OK**.

■ Click **Client control**.

■ Click **Mixed control**, and then click **Customize**.
Configure any of the settings, and then click **OK**.

■ For the Symantec Network Access Control client, you can click **Display the client** and **Display the notification area icon**.

7   Click **OK**.

See "Configuring user interface settings" on page 242.

See "Locking and unlocking Virus and Spyware policy settings" on page 299.

See "Creating a Quarantine policy for a failed Host Integrity check" on page 825.

Configuring user interface settings

You can configure user interface settings on the client if you do either of the following tasks:

■ Set the client's user control level to server control.

■ Set the client's user control level to mixed control and set the parent feature on the Client/Server Control Settings tab to Server.
For example, you can set the Show/Hide notification area icon option to Client. The notification area icon appears on the client and the user can choose to show or hide the icon. If you set the Show/Hide notification area icon option to Server, you can choose whether to display the notification area icon on the client.

To configure user interface settings in mixed control

1   Change the user control level to mixed control.

See "Changing the user control level" on page 239.

2   In the **Client User Interface Control Settings for *location name*** dialog box, next to **Mixed control**, click **Customize**.

3   In the **Client User Interface Mixed Control Settings** dialog box, on the **Client/Server Control Settings** tab, do one of the following actions:

■ Lock an option so that you can configure it only from the server. For the option you want to lock, click **Server**.

Any Virus and Spyware Protection settings that you set to Server here override the settings on the client.

■ Unlock an option so that the user can configure it on the client. For the option you want, click **Client**. Client is selected by default for all settings except the virus and spyware settings.

4 For the following options that you set to **Server**, click the **Client User Interface Settings** tab to configure them:

Show/Hide notification area icon	Display the notification area icon
Enable/Disable Network Threat Protection	Allow users to enable and disable Network Threat Protection
Test Network Security menu command	Allow users to perform a security test
Configure unmatched IP traffic settings	Allow IP traffic or only application traffic, and prompt the user before allowing application traffic
Show/Hide Intrusion Prevention Notifications	Display Intrusion Prevention notifications

For information on where in the console you configure the remaining options that you set to Server, click **Help**. To enable firewall settings and intrusion prevention settings, configure them in the Firewall policy and Intrusion Prevention policy.

See "Automatically allowing communications for essential network services" on page 420.

See "Detecting potential attacks and spoofing attempts" on page 423.

See "Enabling or disabling network intrusion prevention or browser intrusion prevention" on page 467.

5 On the **Client User Interface Settings** tab, check the option's check box so that the option is available on the client.

6 Click **OK**.

7 Click **OK**.

To configure user interface settings in server control

1 Change the user control level to mixed control.

See "Changing the user control level" on page 239.

2 In the Client User Interface Control Settings for *location name* dialog box, next to **Server control**, click **Customize**.

3   In the Client User Interface Settings dialog box, check an option's check box so that the option appears on the client for the user to use.

4   Click **OK**.

5   Click **OK**.

Collecting user information

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

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

See "Managing client installation packages" on page 150.

To collect user information

1   In the console, click **Admin**, and then click **Install Packages**.

2   Under **View Install Packages**, click **Client Install Packages**.

3   In the **Client Install Packages** pane, click the package for which you want to collect user information.

4   Under **Tasks**, click **Set User Information Collection**.

5   In the **Set User Information Collection** dialog box, check **Collect User Information**.

6   In the **Pop-up Message** text box, type the message that you want users to read when they are prompted for information.

7   If you want the user to have the ability to postpone user information collection, check **Enable Remind Me Later**, and then set a time in minutes.

8   Under **Select the fields that will be displayed for the user to provide input**, choose the type of information to collect, and then click **Add**.

      You can select one or more fields simultaneously by pressing the Shift key or the Control key.

9   In the Optional column, check the check box next to any fields that you want
     to define as optional for the user to complete.

10   Click **OK**.

Password-protecting the client

You can increase corporate security by requiring password protection on the client
computer whenever users perform certain tasks.

You can require the users to type a password when users try to do one of the
following actions:

■   Open the client's user interface.

■   Stop the client.

■   Import and export the security policy.

■   Uninstall the client.

You can modify password protection settings only for the subgroups that do not
inherit from a parent group.

See "About access to the client interface" on page 237.

To password-protect the client

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

2   Under **Clients**, select the group for which you want to set up password
     protection.

3   On the **Policies** tab, under **Location-independent Policies and Settings**, click
     General Settings.

4   Click **Security Settings**.

5   On the **Security Settings** tab, under **Client Password Protection**, click any
     of the check boxes.

6   In the **Password** and **Confirm password** text boxes, type the password.

     The password is limited to 15 characters or less.

7   Click **OK**.

Managing remote clients

This chapter includes the following topics:

Managing remote clients

Your network may include some clients that connect to the network from different locations. You may need to manage these clients differently from the clients that connect only from within the network. You may need to manage some clients that always connect remotely over a VPN, or clients that connect from multiple locations because employees travel. You may also need to manage security for some computers that are outside your administrative control. For example, you may allow customers, contractors, vendors, or business partners to have limited

access to your network. Some employees may connect to your network using their own personal computers, and you may need to manage these clients differently.

In all these cases, you must deal with greater security risk. Connections may be less secure, or the client computers may be less secure, and you may have less control over some clients. To minimize these risks to your overall network security, you should assess the different kinds of remote access that clients have to your network. You can then apply more stringent security policies based on your assessment.

To manage the clients that connect to your network differently because of the security risks that they pose, you can work with Symantec Endpoint Protection's location awareness.

You apply different policies to clients that pose a greater risk to your network based on their location. A location in Symantec Endpoint Protection is defined as the type of connection that a client computer uses to connect to your network. A location can also include information about whether the connection is located inside or outside your corporate network.

You define locations for a group of clients. You then assign different policies to each location. Some security settings can be assigned to the entire group regardless of location. Some settings are different depending on location.

Table 12-1   Managing remote clients

Task	Description
Set up groups based on assessment of security risk	See "Managing groups of clients" on page 207.
Set up locations for groups of remote clients	See "Managing locations for remote clients" on page 249.
Configure communication settings for locations	See "Configuring communication settings for a location" on page 259.
Strengthen your security policies	See "About strengthening your security policies for remote clients" on page 260.
Turn on client notifications	See "About turning on notifications for remote clients" on page 262.
Customize client log management settings	See "About customizing log management settings for remote clients" on page 262.
Monitor remote clients	See "About monitoring remote clients" on page 263.

Managing locations for remote clients

You add locations after you set up the groups that you need to manage. Each group can have different locations if your security strategy requires it. In the Symantec Endpoint Protection Manager console, you set up the conditions that trigger automatic policy switching based on location. Location awareness automatically applies the security policy that you specify to a client, based on the location conditions that the client meets.

Location conditions can be based on a number of different criteria. These criteria include IP addresses, type of network connection, whether the client computer can connect to the management server, and more. You can allow or block client connections based on the criteria that you specify.

A location applies to the group you created it for and to any subgroups that inherit from the group. A best practice is to create the locations that any client can use at the My Company group level. Then, create locations for a particular group at the subgroup level.

It is simpler to manage your security policies and settings if you create fewer groups and locations. The complexity of your network and its security requirements, however, may require more groups and locations. The number of different security settings, log-related settings, communications settings, and policies that you need determines how many groups and locations you create.

Some of the configuration options that you may want to customize for your remote clients are location-independent. These options are either inherited from the parent group or set independently. If you create a single group to contain all remote clients, then the location-independent settings are the same for the clients in the group.

The following settings are location-independent:

- Custom intrusion prevention signatures
- System Lockdown settings
- Network application monitoring settings
- LiveUpdate content policy settings
- Client log settings
- Client-server communications settings
- General security-related settings, including location awareness and Tamper Protection

To customize any of these location-independent settings, such as how client logs are handled, you need to create separate groups.

Some settings are specific to locations.

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

■ Auto-Protect

■ SONAR

■ For legacy clients, TruScan proactive threat scans

■ Tamper Protection

■ The firewall rules that you have created

Table 12-2 Location awareness tasks that you can perform

Tasks	Description
Plan locations	You should consider the different types of security policies that you need in your environment to determine the locations that you should use. You can then determine the criteria to use to define each location. It is a best practice to plan groups and locations at the same time. See "Managing groups of clients" on page 207. You may find the following examples helpful: See "Setting up Scenario One location awareness conditions" on page 254. See "Setting up Scenario Two location awareness conditions" on page 256.
Enable location awareness	To control the policies that are assigned to clients contingent on the location from which the clients connect, you can enable location awareness. See "Enabling location awareness for a client" on page 251.
Add locations	You can add locations to groups. See "Adding a location to a group" on page 252.

Table 12-2   Location awareness tasks that you can perform *(continued)*

Tasks	Description
Assign default locations	All groups must have a default location. When you install the console, there is only one location, called Default. When you create a new group, its default location is always Default. You can change the default location later after you add other locations.
	The default location is used if one of the following cases occurs:
	■ One of the multiple locations meets location criteria and the last location does not meet location criteria.
	■ You use location awareness and no locations meet the criteria.
	■ The location is renamed or changed in the policy. The client reverts to the default location when it receives the new policy.
	See "Changing a default location" on page 253.
Configure communications settings for locations	You can also configure the communication settings between a management server and the client on a location basis.
	See "Configuring communication settings for a location" on page 259.

See the knowledge base article Best Practices for Symantec Endpoint Protection Location Awareness.

See "Configuring communication settings for a location" on page 259.

See "Managing remote clients" on page 247.

Enabling location awareness for a client

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

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

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

To enable location awareness for a client

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

2   On the **Clients** page, under **Clients**, select the group for which you want to implement automatic switching of locations.

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

4   Under **Location-independent Policies and Settings**, click **General Settings**.

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

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

6   Check **Enable Location Awareness**.

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

7   Click **OK**.

See "Managing locations for remote clients" on page 249.

See "Adding a location to a group" on page 252.

Adding a location to a group

When you add a location to a group, you specify the conditions that trigger the clients in the group to switch to the location. Location awareness is effective only if you also apply appropriate policies and settings to each location.

To add a location to a group

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

2   In the **Clients** page, under **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 a parent group.

    You can also click **Add Location** to run the **Add Location** wizard.

4   In the **Client** page, under **Tasks**, click **Manage Locations**.

5   In the **Manage Locations** dialog box, under **Locations**, click **Add**.

6   In the **Add Location** dialog box, type the name and description of the new location, and then click **OK**.

7   To the right of the **Switch to this location when** box, click **Add**.

8   In the **Type** list, select a condition, and then select the appropriate definition for the condition.

    A client computer switches to the location if the computer meets the specified criteria.

9   Click **OK**.

10 To add more conditions, click **Add**, and then select either **Criteria with AND relationship** or **Criteria with OR relationship**.

11 Repeat steps 8 through 9.

12 Click **OK**.

See "Managing groups of clients" on page 207.

See "About strengthening your security policies for remote clients" on page 260.

Changing a default location

When the Symantec Endpoint Protection Manager is initially installed, only one location, called Default, exists. At that time, every group's default location is Default. Every group must have a default location. When you create a new group, the Symantec Endpoint Protection Manager console automatically makes its default location Default.

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

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

- One of the multiple locations meets location criteria and the last location does not meet location criteria.

- You use location awareness and no locations meet the criteria.

- The location is renamed or changed in the policy. The client reverts to the default location when it receives the new policy.

To change a default location

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

2   On the **Clients** page, under **Clients,** click the group to which you want to assign a different default location.

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

4   Under **Tasks**, click **Manage Locations**.

5   In the **Manage Locations** dialog box, under **Locations**, select the location that you want to be the default location.

6   Under **Description**, check **Set this location as the default location in case of conflict**.

    The Default location is always the default location until you assign another one to the group.

7   Click **OK**.

See "Managing locations for remote clients" on page 249.

Setting up Scenario One location awareness conditions

If you have remote clients, in the simplest case, it is a common practice to use the My Company group and three locations. This is Scenario One.

To manage the security of the clients in this scenario, you can create the following locations under the My Company group to use:

- Office clients that log on in the office.

- The remote clients that log on to the corporate network remotely over a VPN.

■ The remote clients that log on to the Internet remotely, but not over a VPN.

Because the remote location with no VPN connection is the least secure, it has the most secure policies. It is a best practice to always make this location the default location.

Note: If you turn off My Company group inheritance and then you add groups, the added groups do not inherit the locations that you set up for the My Company group.

The following suggestions represent the best practices for Scenario One.

To set up the office location for the clients located in the office

1   On the **Clients** page, select the group that you want to add a location for.

2   On the **Policies** tab, under **Tasks**, click **Add Location**.

3   In the **Add Location Wizard**, click **Next**.

4   Type a name for the location and optionally, add a description of it, and then click **Next**.

5   In the list box, click **Client can connect to management server** from the list, and then click **Next**.

6   Click **Finish**, and then click **OK**.

7   Under **Tasks**, click **Manage Locations**, and then select the location you created.

8   Click **Add**, and then click **Criteria with AND relationship**.

9   In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.

10 Click **If the client computer does not use the network connection type specified below**.

11 In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.

12 Click **OK** to exit the **Manage Locations** dialog box.

To set up the remote location for the clients logging in over a VPN

1   On the **Clients** page, select the group that you want to add a location for.

2   On the **Policies** tab, under **Tasks**, click **Add Location**.

3   In the **Add Location Wizard**, click **Next**.

4 Type a name for the location and optionally, add a description of it, and then click **Next**.

5 In the list box, click **Network connection type**.

6 In the **Connection Type** list box, select the name of the VPN client that your organization uses, and then click **Next**.

7 Click **Finish**.

8 Click **OK**.

To set up the remote location for the clients not logging on over a VPN

1 On the **Clients** page, select the group that you want to add a location for.

2 On the **Policies** tab, under **Tasks**, click **Add Location**.

3 In the **Add Location Wizard**, click **Next**.

4 Type a name for the location, optionally add a description of it, and then click **Next**.

5 In the list box, leave **No specific condition**, and then click **Next**.

By using these settings, this location's policies, which should be the strictest and most secure, are used as the default location policies.

6 Click **Finish**, and then click **OK**.

See "Setting up Scenario Two location awareness conditions" on page 256.

See "Managing remote clients" on page 247.

Setting up Scenario Two location awareness conditions

In Scenario Two, you use the same two remote locations as specified in Scenario One and two office locations, for a total of four locations.

You would add the following office locations:

■ Clients in the office that log on over an Ethernet connection.

■ Clients in the office that log on over a wireless connection.

It simplifies management to leave all clients under the default server control mode. If you want granular control over what your users can and cannot do, an experienced administrator can use mixed control. A mixed control setting gives the end user some control over security settings, but you can override their changes, if necessary. Client control allows users a wider latitude in what they can do and so constitutes a greater risk to network security.

We suggest that you use client control only in the following situations:

■ If your users are knowledgeable about computer security.

■ If you have a compelling reason to use it.

Note: You may have some clients that use Ethernet connections in the office while other clients in the office use wireless connections. For this reason, you set the last condition in the procedure for wireless clients in the office. This condition lets you create an Ethernet location Firewall policy rule to block all wireless traffic when both kinds of connections are used simultaneously.

To set up the office location for the clients that are logged on over Ethernet

1   On the **Clients** page, select the group that you want to add a location for.

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

3   In the **Add Location Wizard**, click **Next**.

4   Type a name for the location, optionally add a description of it, and then click **Next**.

5   In the list box, select **Client can connect to management server**, and then click **Next**.

6   Click **Finish**.

7   Click **OK**.

8   Under **Tasks**, click **Manage Locations**, and then select the location you created.

9   Beside **Switch to this location when**, click **Add**, and then select **Criteria with AND relationship**.

10 In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.

11 Click **If the client computer does not use the network connection type specified below**.

12 In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.

13 Click **Add** and then click **Criteria with AND relationship**.

14 In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.

15 Click **If the client computer uses the network connection type specified below**.

16 In the bottom list box, select **Ethernet**, and then click **OK**.

17 Click **OK** to exit the Manage Locations dialog box.

To set up the office location for the clients that are logged on over a wireless connection

1 On the **Clients** page, select the group that you want to add a location for.

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

3 In the **Add Location Wizard**, click **Next**.

4 Type a name for the location, optionally add a description of it, and then click **Next**.

5 In the list box, click **Client can connect to management server**, and then click **Next**.

6 Click **Finish**.

7 Click **OK**.

8 Under Tasks, click **Manage Locations**, and then select the location that you created.

9 Beside Switch to this location when, click **Add**, and then click **Criteria with AND relationship**.

10 In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.

11 Click **If the client computer does not use the network connection type specified below**.

12 In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.

13 Click **Add**, and then click **Criteria with AND relationship**.

14 In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.

15 Click **If the client computer does not use the network connection type specified below**.

16 In the bottom list box, click **Ethernet**, and then click **OK**.

17 Click **Add**, and then click **Criteria with AND relationship**.

18 In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.

19 Click **If the client computer uses the network connection type specified below**.

20 In the bottom list box, click **Wireless**, and then click **OK**.

21 Click **OK** to exit the **Manage Locations** dialog box.

See "Setting up Scenario One location awareness conditions" on page 254.

See "Managing remote clients" on page 247.

Configuring communication settings for a location

By default, you configure communication settings between the management server and the client at the level of the group. However, you can also configure these settings for individual locations in a group. For example, you can use a separate management server for a location where the client computers connect through the VPN. To minimize the number of clients that connect to the management server at the same time, you can specify a different heartbeat for each location.

You can configure the following communication settings for locations:

■ The control mode in which the clients run.

■ The management server list that the clients use.

■ The download mode in which the clients run.

■ Whether to collect a list of all the applications that are executed on clients and send the list to the management server.

■ The heartbeat interval that clients use for downloads.

■ Whether the management server randomizes content downloads from the default management server or a Group Update Provider.

Note: Only some of these settings can be configured for Mac clients.

To configure communication settings for a location

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

2 On the **Clients** page, select a group.

3 On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.

4 To the right of **Communications Settings**, click **Tasks**, and then uncheck **Use Group Communications Settings**.

5 Click **Tasks** again, and then click **Edit Settings**.

6   In the **Communications Settings for *location name*** dialog box, modify the settings for the specified location only.

7   Click **OK**.

See "Configuring push mode or pull mode to update client policies and content" on page 308.

See "Managing locations for remote clients" on page 249.

See "Managing groups of clients" on page 207.

About strengthening your security policies for remote clients

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

- Leave the default policies in place, so that you do not impede remote users in the use of their computers.

- Strengthen your default security policies to provide more protection for your network, even if it restricts what remote users can do.

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

Policies may be created as shared or unshared and assigned either to groups or to locations. A shared policy is one that applies to any group and location and can be inherited. A non-shared policy is one that only applies to a specific location in a group. Typically, it is considered a best practice to create shared policies because it makes it easier to change policies in multiple groups and locations. However, when you need unique location-specific policies, you need to create them as non-shared policies or convert them to non-shared policies.

See "Managing remote clients" on page 247.

Best practices for Firewall policy settings

Table 12-3 describes scenarios and best-practice recommendations.

Table 12-3   Firewall policy best practices

Scenario	Recommendation
Remote location where users log on without a VPN	■ Assign the strictest security policies to clients that log on remotely without using a VPN. ■ Enable NetBIOS protection. **Note:** Do not enable NetBIOS protection for the location where a remote client is logged on to the corporate network through a VPN. This rule is appropriate only when remote clients are connected to the Internet, not to the corporate network. ■ Block all local TCP traffic on the NetBIOS ports 135, 139, and 445 to increase security.
Remote location where users log on through a VPN	■ Leave as-is all the rules that block traffic on all adapters. Do not change those rules. ■ Leave as-is the rule that allows VPN traffic on all adapters. Do not change that rule. ■ Change the Adapter column from All Adapters to the name of the VPN adapter that you use for all rules that use the action Allow. ■ Enable the rule that blocks all other traffic. **Note:** You need to make all of these changes if you want to avoid the possibility of split tunneling through the VPN.
Office locations where users log on through Ethernet or wireless connections	Use your default Firewall policy. For the wireless connection, ensure that the rule to allow wireless EAPOL is enabled. 802.1x uses the Extensible Authentication Protocol over LAN (EAPOL) for connection authentication.

See "Creating a firewall policy" on page 416.

See "Automatically allowing communications for essential network services" on page 420.

About best practices for LiveUpdate policy settings

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

For the remote location where users log in without a VPN, we suggest the following best practices:

- Change the LiveUpdate policy setting to use the default Symantec LiveUpdate server. This setting allows the remote clients to update any time they connect to the Internet.

- Change the LiveUpdate Scheduling frequency setting to one hour to make it more likely that clients update their protection when they connect to the Internet.

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

See "Managing remote clients" on page 247.

About turning on notifications for remote clients

For your remote clients that are not logged on over VPN, it is a best practice to turn on client notifications for the following situations:

- Intrusion detections
  You can turn on these notifications by using the location-specific server or, you can select the **Mixed control** option in the **Client User Interface Control Settings**. You can customize the settings on the **Client User Interface Settings** tab.

- Virus and security risks
  You can turn on these notifications in the Virus and Spyware Protection policy.

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

See "Managing remote clients" on page 247.

About customizing log management settings for remote clients

You may want to customize the log management settings for remote clients. Customization can be especially useful if clients are offline for several days.

The following settings can help reduce bandwidth and the load on your management servers:

- Clients do not upload their logs to the management server.

- Clients upload only the client security logs.

- Filter log events to upload only specified events.
  Suggested events to upload include definition updates, or side effect repair
  failures.

- Make the log retention time longer.
  Longer retention times let you review more antivirus and antispyware event
  data.

Note: Some client log settings are specific to a group. Location-specific log settings
are part of a Virus and Spyware Protection policy. Depending on the log settings
that you want to customize, you may need to use groups instead of locations to
manage your remote clients.

See "Viewing logs" on page 624.

About monitoring remote clients

Notifications and logs are essential to maintain a secure environment. In general,
you should monitor your remote clients in the same way that you monitor your
other clients. You should always check to see that your protections are up to date
and that your network is not currently under attack. If your network is under
attack, then you want to find out who is behind the attack and how they attacked.

Your Home page preference settings determine the time period for which Symantec
Endpoint Protection Manager displays data. By default, the data on the Home
page represents only the clients that connected in the past 12 hours. If you have
many clients that are frequently offline, your best monitoring option is to go to
the logs and reports. In the logs and reports, you can filter the data to include
offline clients.

Even if you restrict some of the client log data that mobile clients upload, you can
check the following displays.

	Table 12-4	Displays to monitor remote client security

Display	Description
Home > Endpoint Status	Displays whether the content is up to date or to see if any of the protections are turned off.
	You can check the following status conditions:
	■ Content dates and version numbers
	■ Client connections
	■ Enabled and disabled protections
	You can click **Details** to see the status for each client.
Home > Security Status	Displays the system security overview. View the **Virus and Risks Activity Summary** to see if your network is under attack.
	You can click **Details** to see the status for each security protection technology.
Home > Virus and Risks Activity Summary	Displays the detected virus and risk activity, and the actions taken, such as cleaned, blocked, or quarantined.
Monitors > Summary Type > Network Threat Protection	Displays the information about attack types and sources.

See "Managing remote clients" on page 247.

Managing domains

This chapter includes the following topics:

- About domains

- Adding a domain

- Switching to the current domain

About domains

When you install a management server, the Symantec Endpoint Protection Manager console includes one domain, which is called Default. A domain is a structural container in the console that you use to organize a hierarchy of groups, clients, computers, and policies. You set up additional domains to manage your network resources.

Note: The domains in Symantec Endpoint Protection Manager do not relate to Microsoft domains.

Each domain that you add shares the same management server and database, and it provides an additional instance of the console. All data in each domain is completely separate. This separation prevents administrators in one domain from viewing data in other domains. You can add an administrator account so that each domain has its own administrator. These administrators can view and manage only the contents of their own domain.

If your company is large, with sites in multiple regions, you may need to have a single view of management information. You can delegate administrative authority, physically separate security data, or have greater flexibility in how users, computers, and policies are organized. If you are a managed service provider (MSP), you may need to manage multiple independent companies, as well as

Internet service providers. To meet these needs, you can create multiple domains. For example, you can create a separate domain for each country, region, or company.

Figure 13-1 Overview of Symantec Endpoint Protection Manager domains
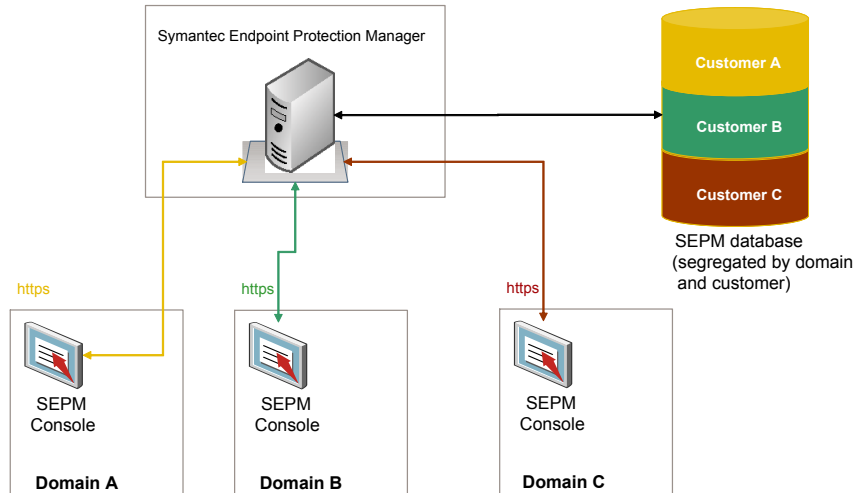
When you add a domain, the domain is empty. You must set the domain to be the current domain. You then add groups, clients, computers, and policies to this domain.

You can copy policies and clients from one domain to another. To copy policies between domains, you export the policy from the originating domain and you import the policy into the destination domain. To copy clients between domains, you use the SylinkDrop tool. This tool replaces the communication file on a client to allow the client to talk to a different management server.

You can disable a domain if you no longer need it. Ensure that it is not set as the current domain when you attempt to disable it.

See "Adding a domain" on page 267.

See "Restoring client-server communication settings by using the SylinkDrop tool" on page 764.

See "Switching to the current domain" on page 267.

Adding a domain

You create a domain to organize a hierarchy of groups, users, clients, and policies in your organization. For example, you may want to add domains to organize users by division.

Note: You can use a domain ID for disaster recovery. If all the management servers in your organization fail, you need to rebuild the management server by using the same ID as the old server. You can get the old domain ID from the sylink.xml file on any client.

To add a domain

1　In the console, click **Admin**.

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

3　Under Tasks, click **Add Domain**.

4　In the Add Domain dialog box, type a domain name, an optional company name, and optional contact information.

5　If you want to add a domain ID, click **Advanced** and then type the value in the text box.

6　Click **OK**.

See "About domains" on page 265.

Switching to the current domain

The default domain name is **Default**, and it is set as the current domain. When you add a new domain in the Symantec Endpoint Protection Manager console, the domain is empty. To add groups, clients, policies, and administrators to a new domain, you must first set it as the current domain. When a domain is designated as the current domain, the text **Current Domain** follows the domain name in the title. If you have many domains, you must scroll through the **Domains** list to display which domain is the current one.

If you logged on to the console as a system administrator, you can see all domains no matter which domain is the current one. However, you can only see the administrators and limited administrators that were created in the current domain. If you logged on to the console as either an administrator or a limited administrator, you only see the domain to which you have access.

If you remove the current domain, the management server logs you out. You can only remove a domain if it is not the current domain and not the only domain.

To switch to the current domain

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

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

3   Under **Domains**, click the domain that you want to make the current domain.

4   Under **Tasks**, click **Administer Domain**.

5   In the Administer Domain dialog box, to confirm, click **Yes**.

6   Click **OK**.

See "About domains" on page 265.

See "Adding a domain" on page 267.

Managing administrator accounts and passwords

This chapter includes the following topics:

Managing domains and administrator accounts

You can use administrator accounts to manage Symantec Endpoint Protection Manager. Administrators log on to the Symantec Endpoint Protection Manager console to change policy settings, manage groups, run reports, and install client software, as well as other management tasks.

The default account is a system administrator account, which provides access to all features. You can also add a more limited administrator account, for administrators who need to perform a subset of tasks.

For a small company, you may only need one administrator. For a large company with multiple sites and domains, you most likely need multiple administrators, some of whom have more access rights than others.

You manage domains and administrator accounts and their passwords on the **Admin** page.

Table 14-1   Account and domain administration

Task	Description
Decide whether to add multiple domains	Decide whether to add domains. See "About domains" on page 265. See "Adding a domain" on page 267. See "Switching to the current domain" on page 267.
Add administrator accounts	Add accounts for administrators who need access to the Symantec Endpoint Protection Manager console. ■ Learn about the administrator account roles that are available. See "About administrator account roles and access rights" on page 271. ■ Create the types of administrator accounts that you need. See "Adding an administrator account" on page 273. See "Configuring the access rights for a limited administrator" on page 274. ■ Change the method that is used to authenticate administrator accounts (optional). By default, the Symantec Endpoint Protection Manager database authenticates the administrator's credentials. You can also use RSA SecurID or an LDAP server or a Microsoft Active Directory Server for authentication. See "Changing the authentication method for administrator accounts" on page 275.
Unlock or lock an administrator account	By default, Symantec Endpoint Protection Manager locks out an administrator after a user tries to log on to Symantec Endpoint Protection Manager using the administrator account too many times. You can configure these settings to increase the number of tries or time the administrator is locked out. See "Unlocking an administrator's account after too many logon attempts" on page 104.

	Table 14-1	Account and domain administration *(continued)*

Task	Description
Reset passwords	You can perform the following tasks for passwords: ■ Change the password for an administrator account. See "Changing the password for an administrator account" on page 283. ■ Make sure that the **Forget your password?** link appears so that administrators can reset their own forgotten passwords. See "Allowing administrators to reset forgotten passwords" on page 284. ■ Send an administrator a temporary password so that they can reset their password. ■ Display the **Remember my user name** and **Remember my password** check boxes on the management server log on screen. See "Displaying the Remember my user name and Remember my password check boxes on the logon screen" on page 286.
Configure log on options for Symantec Endpoint Protection Manager	You can configure the following log on options for each type of administrator: ■ Display a message for administrators to read before they log on. See "Displaying a message for administrators to see before logging on Symantec Endpoint Protection Manager" on page 101. ■ Allow or block log on access to the management console, so that certain administrators can, or cannot, log on remotely. See "Granting or blocking access to remote Symantec Endpoint Protection Manager consoles" on page 102. ■ By default, if an administrator tries to log on to Symantec Endpoint Protection Manager too many times, the administrator is locked out for 15 minutes. You can configure these settings for each administrator. See "Unlocking an administrator's account after too many logon attempts" on page 104.

See "Logging on to the Symantec Endpoint Protection Manager console" on page 99.

About administrator account roles and access rights

When you install the Symantec Endpoint Protection Manager, a default system administrator account is created, called `admin`. The system administrator account gives an administrator access to all the features in Symantec Endpoint Protection Manager.

To help you manage security, you can add additional system administrator accounts, domain administrator accounts, and limited administrator accounts. Domain administrators and limited administrators have access to a subset of Symantec Endpoint Protection Manager features.

You choose which accounts you need based on the types of roles and access rights you need in your company. For example, a large company may use the following types of roles:

- An administrator who installs the management server and the client installation packages. After the product is installed, an administrator in charge of operations takes over. These administrators are most likely system administrators.

- An operations administrator maintains the servers, databases, and installs patches. If you have a single domain, the operations administrator could be a domain administrator who is fully authorized to manage sites.

- An antivirus administrator, who creates and maintains the Virus and Spyware policies and LiveUpdate policies on the clients. This administrator is most likely to be a limited administrator.

- A desktop administrator, who is in charge of security and creates and maintains the Firewall policies and Intrusion Prevention policies for the clients. This administrator is most likely to be a domain administrator.

- A help desk administrator, who creates reports and has read-only access to the policies. The antivirus administrator and desktop administrator read the reports that the help desk administrator sends. The help desk administrator is most likely to be a limited administrator who is granted reporting rights and policy rights.

Table 14-2 describes the account type and the access rights that each role has.

Table 14-2   Administrator roles and responsibilities

Administrator role	Responsibilities
System administrator	System administrators can log on to the Symantec Endpoint Protection Manager console with complete, unrestricted access to all features and tasks.
	A system administrator can create and manage other system administrator accounts, domain administrator accounts, and limited administrator accounts.
	A system administrator can perform the following tasks:
	■ Manage all domains.
	■ Administer licenses.
	■ View and manage all console settings.
	■ Manage the databases and management servers.
	■ Manage Enforcers.

Administrator role	Responsibilities
Administrator	Administrators are domain administrators who can view and manage a single domain. A domain administrator has the same privileges as a system administrator, but for a single domain only.
	By default, the domain administrator has full system administrator rights to manage a domain, but not a site. You must explicitly grant site rights within a single domain. Domain administrators can modify the site rights of other administrators and limited administrators, though they cannot modify the site rights for themselves.
	A domain administrator can perform the following tasks:
	■ Create and manage administrator accounts and limited administrator accounts within a single domain. Domain administrators cannot modify their own site rights. System administrators must perform this function.
	■ Run reports, manage sites, and reset passwords. You must explicitly configure reporting rights to groups that are migrated from Symantec AntiVirus 10.x.
	■ Cannot administer licenses. Only system administrators can administer licenses.
	■ Cannot manage Enforcers.
	See "About domains" on page 265.
Limited administrator	Limited administrators can log on to the Symantec Endpoint Protection Manager console with restricted access. Limited administrators do not have access rights by default. A system administrator role must explicitly grant access rights to allow a limited administrator to perform tasks.
	Parts of the management server user interface are not available to limited administrators when you restrict access rights. For example:
	■ Limited administrators without reporting rights cannot view the **Home**, **Monitors**, or **Reports** pages.
	■ Limited administrators without policy rights cannot view or modify the policy. In addition, they cannot apply, replace, or withdraw a policy.
	See "Configuring the access rights for a limited administrator" on page 274.

See "Managing domains and administrator accounts" on page 269.

See "Adding an administrator account" on page 273.

Adding an administrator account

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 with access rights equal to or less restrictive

than your own. Administrators can add limited administrators and configure their access rights.

To add an administrator account

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

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

3   Under **Tasks**, click **Add an administrator**.

4   In the **Add Administrator** dialog box, on the **General** tab, enter the user name and email address.

5   On the **Access Rights** and **Authentication** tabs, specify the administrator role, access rights, and authentication method.

See "About administrator account roles and access rights" on page 271.

See "Changing the authentication method for administrator accounts" on page 275.

Click **Help** for more information.

6   Click **OK**.

See "Managing domains and administrator accounts" on page 269.

Configuring the access rights for a limited administrator

If you add an account for a limited administrator, you must also specify the administrator's access rights. Limited administrator accounts that are not granted any access rights are created in a disabled state and the limited administrator will not be able to log on to the management server.

Note: Reporting rights are required to integrate Symantec Endpoint Protection Manager with Symantec Protection Center version 1. Ensure that you grant reporting rights to any limited administrators who use Protection Center version 1 to access the Symantec Endpoint Protection Manager console. For more information, see the Help for Protection Center version 1.

To configure the access rights for a limited administrator

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

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

3   Select the limited administrator.

You can also configure the access rights when you create a limited administrator account.

See "Adding an administrator account" on page 273.

4   Under **Tasks**, click **Edit Administrator**.

5   On the **Access Rights** tab, check an option, and then click the corresponding button to set the access rights. Click **Help** for more information.

6   If you want to authorize the limited administrator to create only non-shared policies for a location, check **Only allow location-specific policy editing**.

7   Click **OK**.

See "About administrator account roles and access rights" on page 271.

See "Managing domains and administrator accounts" on page 269.

Changing the authentication method for administrator accounts

After you add an administrator account, the user name and password are stored in the Symantec Endpoint Protection Manager database. When the administrator logs on to the management server, the management server verifies with the database that the user name and password are correct. However, if your company uses a third-party server to authenticate existing user names and passwords, you can configure Symantec Endpoint Protection Manager to authenticate with the server.

Table 14-3 displays the authentication methods the management server can use to authenticate administrator accounts.

Table 14-3   Authentication methods

Symantec Endpoint Protection Manager authentication (default)	Authenticates the administrators with the administrator's the credentials that are stored in the Symantec Endpoint Protection Manager database.
RSA SecurID authentication	Authenticates the administrators by using RSA SecurID token (not software RSA tokens), RSA SecurID card, or RSA keypad card (not RSA smart cards).
Directory server authentication	Authenticates the administrators with an LDAP server or the Microsoft Active Directory server.

For the third-party authentication methods, Symantec Endpoint Protection Manager has an entry in the database for the administrator account, but the third-party server validates the user name and password.

To change the authentication method for administrator accounts

1   Add an administrator account.

    See "Adding an administrator account" on page 273.

2   On the **Authentication** tab, select the authentication method.

    ■   To authenticate administrators who use an RSA SecurID mechanism, first install the RSA ACE server and enable encrypted authentication for RSA SecurID.
    See "Configuring the management server to authenticate administrators who use RSA SecurID to log on" on page 277.
    See "Authenticating administrators who use RSA SecurID to log on to the management server" on page 278.

    ■   To authenticate administrators using an Active Directory or LDAP directory server, you need to set up an account on the directory server. You must also establish a connection between the directory server and Symantec Endpoint Protection Manager. If you do not establish a connection, you cannot import users from an Active Directory server or synchronize with it.

    Note: Synchronization is only possible for Active Directory Servers. Symantec Endpoint Protection does not support synchronization with LDAP servers.

    You can check whether the directory server authenticates the account name by clicking **Test Account**.
    See "Connecting Symantec Endpoint Protection Manager to a directory server" on page 213.
    See "Best practices for testing whether a directory server authenticates an administrator account" on page 278.

3   Click **OK**.

4   In the **Confirm Change** dialog box, type the password that you use to log on to Symantec Endpoint Protection Manager, and then click **OK**.

    When you switch between authentication methods, you must type the administrator account's password.

Configuring the management server to authenticate administrators who use RSA SecurID to log on

If your corporate network includes an RSA server, you need to install the software for an RSA ACE Agent on the computer on which you installed Symantec Endpoint Protection Manager and configure it as a SecurID Authentication client.

To configure the management server to authenticate administrators who use RSA SecurID to log on

1   Install the software for the RSA ACE Agent on the same computer on which you installed the management server. You can install the software by running the Windows .msi file from the RSA Authentication Agent product disc.

2   Copy the nodesecret.rec, sdconf.rec, and agent_nsload.exe files from the RSA ACE server to the computer on which you installed the management server.

3   At the command prompt, type the following command:

    `agent_nsload -f nodesecret.rec -p password`

    where *password* is the password for the `nodesecret` file.

4   In the console, click **Admin**, and then click **Servers**.

5   Under **Servers**, select the management server to which you want to connect an RSA server.

6   Under **Tasks**, click **Configure SecurID authentication**.

7   In the **Welcome to the Configure SecurID Authentication Wizard** panel, click **Next**.

8   In the **Qualification** panel of the **Configure SecurID Authentication Wizard** panel, read the prerequisites so that you can meet all the requirements.

9   Click **Next**.

10 In the **Upload RSA File** panel of the **Configure SecurID Authentication Wizard** panel, browse for the folder in which the sdconf.rec file resides.

    You can also type the path name.

11 Click **Next**.

12 Click **Test** to test your configuration.

13 In the **Test Configuration** dialog box, type the user name and password for your SecurID, and then click **Test**.

    It now authenticates successfully.

See "Authenticating administrators who use RSA SecurID to log on to the management server" on page 278.

Authenticating administrators who use RSA SecurID to log on to the management server

If you want to authenticate administrators who use the Symantec Endpoint Protection Manager with RSA SecurID, you need to enable encrypted authentication by running the RSA installation wizard.

To authenticate administrators who use RSA SecurID to log on to the management server

1 Install an RSA ACE server, if necessary.

2 Register the computer on which you installed the management server as a valid host on the RSA ACE server.

3 Create the Node Secret file for the same host.

4 Ensure that the sdconf.rec file on the RSA ACE server is accessible on the network.

5 Assign a synchronized SecurID card or key fob to a management server account; activate the logon name on the RSA ACE server.

6 Ensure that the administrator has the RSA PIN or password available.

Symantec supports the following types of RSA logons:

■ RSA SecurID token (not software RSA tokens)

■ RSA SecurID card

■ RSA keypad card (not RSA smart cards)

To log on to the management server with the RSA SecurID, the administrator needs a logon name, the token (hardware), and a pin number.

See "Configuring the management server to authenticate administrators who use RSA SecurID to log on" on page 277.

See "Changing the authentication method for administrator accounts" on page 275.

Best practices for testing whether a directory server authenticates an administrator account

You can test whether an Active Directory or LDAP server authenticates the user name and password for an administrator account that you create. The test also ensures that you added the user name and password correctly.

You use the same user name and password for an administrator account in Symantec Endpoint Protection Manager as you do in the directory server. When the administrator logs on to the management server, the directory server

authenticates the administrator's user name and password. The management server uses the directory server configuration that you added to search for the account on the directory server.

The **Test Account** option checks whether or not the account name exists on the directory server.

You can also test whether an Active Directory or LDAP server authenticates an administrator account with no user name and password. An account with no user name or password is anonymous access. You should create an administrator account with anonymous access so that the administrators are never locked out if the password changes on the directory server.

Note: In Windows 2003 Active Directory server, anonymous authentication is disabled by default. Therefore, when you add a directory server without a user name to an administrator account and click **Test Account**, an **Account Authentication Failed** error message appears. To work around this issue, create two directory server entries, one for testing, and one for anonymous access. The administrator can still log on to the management server using a valid user name and password.

Table 14-4   Steps to test directory server authentication for an administrator account

Step	Task	Description
Step 1	Add multiple directory server connections	To make testing easier for anonymous access, add at least two directory server entries. Use one entry to test the authentication, and the second entry to test anonymous access. These entries all use the same directory server with different configurations.
		By default, most users reside in CN=Users unless moved to different organizational unit. Users in the LDAP directory server are created under CN=Users, DC=<*sampledomain*>, DC=local. To find out where a user resides in LDAP, use ADSIEdit.
		Use the following information to set up the directory servers for this example:
		■ CN=John Smith ■ OU=test ■ DC=<*sampledomain*> ■ DC=local
		The example uses the default Active Directory LDAP (389) but can also use Secure LDAP (636).

Table 14-4 Steps to test directory server authentication for an administrator account *(continued)*

Step	Task	Description
Step 2	Add multiple administrator accounts	You add multiple system administrator accounts. The account for anonymous access does not user a user name or password. See "To add the administrator accounts using the directory server entries" on page 281.

To add the directory server connections to test Active Directory and LDAP server authentication

1   On the console, click **Admin** > **Servers**, select the default server, and click **Edit the server properties**.

2   On the **Directory Servers** tab, click **Add**.

3   On the **General** tab, add the following directory server configurations, and then click **OK**.

Directory server 1:

■ **Name:** *<sampledomain>* `Active Directory`

■ **Server Type: Active Directory**

■ **Server IP Address or Name:** `server01.`*<sampledomain>*`.local`

■ **User Name:** *<sampledomain>*`\administrator`

■ **Password:** *<directory server password>*

Directory server 2:

■ **Name:** *<sampledomain>* `LDAP with User Name`

■ **Server Type: LDAP**

■ **Server IP Address or Name:** `server01.`*<sampledomain>*`.local`

■ **LDAP Port: 389**

■ **LDAP BaseDN:** `DC=`*<sampledomain>*`, DC=local`

■ **User Name:** *<sampledomain>*`\administrator`

■ **Password:** *<directory server password>*

Directory server 3 (for anonymous authentication):

■ **Name:** *<sampledomain>* `LDAP without User Name`

■ **Server Type: LDAP**

- ■ **Server IP Address or Name:** `server01.`*`<sampledomain>`*`.local`

- ■ **LDAP Port: 389**

- ■ **LDAP BaseDN:** <empty>
  Leave this field empty when you use anonymous access.

- ■ **User Name:** <empty>

- ■ **Password:** <empty>
  After you click **OK**, a warning appears. But the directory server is valid. When you try to add a BaseDN without a user name and password, the warning appears.

To add the administrator accounts using the directory server entries

1   On the console, click **Admin** > **Administrators**, and on the **General** tab, add the administrator accounts in step 2.

   See "Adding an administrator account" on page 273.

   See "Changing the authentication method for administrator accounts" on page 275.

   After you add each administrator account and click the **Test Account** option, you see a message. In some cases, the message appears to invalidate the account information. But the administrator can log on to Symantec Endpoint Protection Manager.

2   Administrator account 1:

   - ■ On the **General** tab, type add the following information:
     User Name: `john`

   - ■ **Full Name:** `John Smith`

   - ■ **Email Address:** `john@`*`<sampledomain>`*`.local`

   - ■ On the **Access Rights** tab, click **System Administrator**.

   - ■ On the **Authentication** tab, click **Directory Authentication**.
     In the **Directory Server** drop-down list, select *`<sampledomain>`* `Active Directory`.
     In the **Account Name** field, type `john`.
     Click **Test Account**.
     The system administrator `john` can log on to Symantec Endpoint Protection Manager with directory authentication.

   Administrator account 2:

   - ■ On the **General** tab, type add the following information:

- ■ **User Name:** john

- ■ **Full Name:** John Smith

- ■ **Email Address:** john@<*sampledomain*>.local

- ■ On the **Access Rights** tab, click **System Administrator**.

- ■ On the **Authentication** tab, click **Directory Authentication**.
  In the **Directory Server** drop-down list, select <*sampledomain*> LDAP
  with User Name.
  In the **Account Name** field, type john.
  Click **Test Account**.
  The system administrator john cannot log on into Symantec Endpoint
  Protection Manager with directory authentication.

Administrator account 3:

- ■ On the **General** tab, type add the following information:

- ■ **User Name:** john

- ■ **Full Name:** John Smith

- ■ **Email Address:** john@<*sampledomain*>.local

- ■ On the **Access Rights** tab, click **System Administrator**.

- ■ On the **Authentication** tab, click **Directory Authentication**.
  In the **Directory Server** drop-down list, select <*sampledomain*> LDAP
  with User Name.
  In the **Account Name** field, type John Smith.
  Click **Test Account**.
  The system administrator john can log on into Symantec Endpoint
  Protection Manager with directory authentication.

Administrator account 4, for anonymous access:

- ■ On the **General** tab, type add the following information:

- ■ **User Name:** john

- ■ **Full Name:** John Smith

- ■ **Email Address:** john@<*sampledomain*>.local

- ■ On the **Access Rights** tab, click **System Administrator**.

- ■ On the **Authentication** tab, click **Directory Authentication**.
  In the **Directory Server** drop-down list, select <*sampledomain*> LDAP
  without User Name.

In the **Account Name** field, type `John Smith`.

Click **Test Account**.

The account authentication fails, but the system administrator `John Smith` can log on to Symantec Endpoint Protection Manager.

See "Connecting Symantec Endpoint Protection Manager to a directory server" on page 213.

Changing the password for an administrator account

For security purposes, you may need to change the password for another administrator's account.

The following rules apply to changing passwords:

- System administrators can change the password for all administrators.

- Domain administrators can change the password for other domain administrators and limited administrators within the same domain.

- Limited administrators can change their own passwords only.

Note: When you configure the management server in the Management Server Configuration Wizard, you select either the embedded database or a Microsoft SQL Server database. If you select the embedded database, the password you enter for the default administrator account `admin` also becomes the database password. If you change the default administrator's password, the database password does not change.

If the password is reset to fix an administrator account lockout, the administrator must still wait for the lockout period to expire. The default lockout period is 15 minutes.

See "Unlocking an administrator's account after too many logon attempts" on page 104.

To change the password for an administrator account

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

2   Under **Administrators**, select the administrator account, and then click **Change password**.

3   Type both your password and the administrator's new password..

The password must be six to 20 characters in length. The following characters are not allowed: `"/ \ [ ] : ; | = , + * ? < >`

4   Click **Change**.

See "Managing domains and administrator accounts" on page 269.

Allowing administrators to reset forgotten passwords

If you have a system administrator account, you can allow your administrators to reset passwords. If you enable this feature, administrators can click the **Forgot your password?** link on the logon panel to request a temporary password.

Note: You can allow this method to reset a password only for the administrator accounts that authenticate by using Symantec Management Server authentication. This method does not work for any administrator accounts that authenticate by using either RSA SecurID authentication or directory authentication.

To allow administrators to reset forgotten passwords

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

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

3   Under **Servers**, select the local site.

You control this setting only for the local site.

4   Click **Edit Site Properties**.

5   On the **Passwords** tab, check **Allow administrators to reset the passwords**.

6   Click **OK**.

See "Sending a temporary password to an administrator" on page 284.

See "Displaying the Remember my user name and Remember my password check boxes on the logon screen" on page 286.

See "Managing domains and administrator accounts" on page 269.

Sending a temporary password to an administrator

If you have a system administrator account, you can allow your administrators to reset their own passwords. An email that contains a link to activate the temporary password is sent to the administrator. You must first make sure the

Forgot your password? link appears on the Symantec Endpoint Protection Manager log on screen.

For security reasons, the management server does not store or verify the temporary passwords. To verify whether the administrator successfully reset the password, check that the administrator received the email message.

An administrator can request a temporary password from the management console only once per minute.

You must configure the mail server so that the mail server sends the notification.

You can use this method to reset a password only for the administrator accounts that authenticate by using Symantec Management Server authentication. This method does not work for any administrator accounts that authenticate by using either RSA SecurID authentication or directory authentication.

To send a temporary password to an administrator

1   On the management server computer, click **Start** > **All Programs** > **Symantec Endpoint Protection Manager** > **Symantec Endpoint Protection Manager**.

    By default, the **Forgot your password?** link appears on the management server logon screen. If it does not, you must enable it.

    See "Displaying the Remember my user name and Remember my password check boxes on the logon screen" on page 286.

2   In the **Logon** screen, click **Forgot your password?**

3   In the **Forgot Password** dialog box, type the user name for the account for which to reset the password.

    For domain administrators and limited administrators, type the domain name for the account. If you did not set up domains, leave the domain field blank.

4   Click **Temporary Password**.

    As a security precaution, the administrator must change the temporary password immediately after logging on.

See "Establishing communication between the management server and email servers" on page 640.

See "Changing the authentication method for administrator accounts" on page 275.

See "Managing domains and administrator accounts" on page 269.

Displaying the Remember my user name and Remember my password check boxes on the logon screen

You can display the **Remember my user name** and **Remember my password** check boxes on the Symantec Endpoint Protection Manager logon screen. If you enable this feature, the administrator's user name and password is prepopulated on the logon screen.

To display the Remember my user name and Remember my password check boxes on the logon screen

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

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

3   Under **Domains**, select the domain for which to allow administrators to save logon credentials.

4   Click **Edit Domain Properties**.

5   On the **Passwords** tab, check **Allow users to save credentials when logging on**.

6   Click **OK**.

See "Managing domains and administrator accounts" on page 269.

Section 3

Managing protection and customizing policies

Using policies to manage security

This chapter includes the following topics:

- Performing the tasks that are common to all policies

- The types of security policies

- About shared and non-shared policies

- Adding a policy

- Editing a policy

- Copying and pasting a policy on the Policies page

- Copying and pasting a policy on the Clients page

- Locking and unlocking Virus and Spyware policy settings

- Assigning a policy to a group

- Testing a policy

- Replacing a policy

- Exporting and importing individual policies

- Converting a shared policy to a non-shared policy

- Withdrawing a policy from a group

- How the client computers get policy updates

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

- Using the policy serial number to check client-server communication

- Manually updating policies on the client

- Monitoring the applications and services that run on client computers

- Searching for information about the applications that the computers run

Performing the tasks that are common to all policies

Your security policies define how the protection technologies protect your computers from known and unknown threats.

You can manage your Symantec Endpoint Protection security policies in many ways. For example, you can create copies of the security policies and then customize the copies for your specific needs. You can lock and unlock certain settings so that users cannot change them on the client computer.

Table 15-1 describes many of the policy tasks that you can perform.

Table 15-1   Tasks common to all policies

Task	Description
Add a policy	If you do not want to use one of the default policies, you can add a new policy.
	You can add shared policies or non-shared policies.
	Note: If you add or edit shared policies in the **Policies** page, you must also assign the policies to a group or location. Otherwise those policies are not effective.
	See "The types of security policies" on page 293.
	See "About shared and non-shared policies" on page 295.
	See "Adding a policy" on page 296.
Lock and unlock policy settings	You can lock and unlock some **Virus and Spyware Protection policy** settings. Computer users cannot change locked policy settings. A padlock icon appears next to a lockable policy setting.
	See "Locking and unlocking Virus and Spyware policy settings" on page 299.

Table 15-1   Tasks common to all policies *(continued)*

Task	Description
Edit a policy	If you want to change the settings in an existing policy, you can edit it. You can increase or decrease the protection on your computers by modifying its security policies. You do not have to reassign a modified policy unless you change the group assignment. See "Editing a policy" on page 297.
Assign a policy	To put a policy into use, you must assign it to one or more groups or locations. See "Assigning a policy to a group" on page 300.
Test a policy	Symantec recommends that you always test a new policy before you use it in a production environment. See "Testing a policy" on page 301.
Update the policies on clients	Based on the available bandwidth, you can configure a client to use push mode or pull mode as its policy update method. See "How the client computers get policy updates" on page 307. See "Configuring push mode or pull mode to update client policies and content" on page 308.
Replace a policy	You can replace a shared policy with another shared policy. You can replace the shared policy in either all locations or for one location. See "Replacing a policy" on page 302.
Copy and paste a policy	Instead of adding a new policy, you may want to copy an existing policy to use as the basis for the new policy. You can copy and paste policies on either the **Policies** page or the **Policies** tab on the **Clients** page. **Note:** You can also copy all the policies in a group and paste them into another group, from the **Policies** tab on the **Clients** page. See "Copying and pasting a policy on the Clients page" on page 298. See "Copying and pasting a policy on the Policies page" on page 298.

Table 15-1 Tasks common to all policies *(continued)*

Task	Description
Convert a shared policy to a non-shared policy	You can copy the content of a shared policy and create a non-shared policy from that content.
	See "About shared and non-shared policies" on page 295.
	A copy enables you to change the content of a shared policy in one location and not in all other locations. The copy overrides the existing non-shared policy.
	You can convert a shared policy to a non-shared policy if the policy no longer applies to all the groups or all the locations. When you finish the conversion, the converted policy with its new name appears under Location-specific Policies and Settings.
	See "Converting a shared policy to a non-shared policy " on page 304.
Export and import a policy	You can export an existing policy if you want to use it at a different site or management server. You can then import the policy and apply it to a group or to a specific location.
	See "Exporting and importing individual policies" on page 303.
	You can also export and import all policies rather than one policy at a time. If you upgrade the management server from a previous version to a newer version, you should export import all the policies.
	See "Exporting and importing server settings" on page 719.
Withdraw a policy	If you delete a policy, Symantec Endpoint Protection removes the policy from the database. If you do not want to delete a policy, but you no longer want to use it, you can withdraw the policy instead.
	You can withdraw any type of policy except a **Virus and Spyware Protection policy** and a **LiveUpdate Settings policy**.
	See "Withdrawing a policy from a group" on page 305.
Delete a policy	If a policy is assigned to one or more groups and locations, you cannot delete it until you have unassigned it from all the groups and locations. You can also replace the policy with another policy

Table 15-1   Tasks common to all policies *(continued)*

Task	Description
Check that the client has the latest policy	You can check whether the client has the latest policy. If not, you can manually update the policy on the client. See "How the client computers get policy updates" on page 307. See "Using the policy serial number to check client-server communication" on page 309. See "Manually updating policies on the client" on page 310.

The types of security policies

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

See "Performing the tasks that are common to all policies" on page 290.

Table 15-2   Security policy types

Policy type	Description
Virus and Spyware Protection policy	The **Virus and Spyware Protection policy** provides the following protection: ■ Detects, removes, and repairs the side effects of virus and security risks by using signatures. ■ Detects the threats in the files that users try to download by using reputation data from Download Insight. ■ Detect the applications that exhibit suspicious behavior by using SONAR heuristics and reputation data. The **Virus and Spyware Protection policy** finds behavior anomalies through its SONAR technology. For legacy clients, it finds behavior anomalies through TruScan proactive threat scans. **Note:** Download Insight and SONAR technology are available only on Windows clients. See "Managing scans on client computers" on page 323.

Table 15-2 Security policy types *(continued)*

Policy type	Description
Firewall policy	The **Firewall policy** provides the following protection: ■ Blocks the unauthorized users from accessing the computers and networks that connect to the Internet. ■ Detects the attacks by hackers. ■ Eliminates the unwanted sources of network traffic. **Note:** Firewall policies can be applied only to Windows clients. See "Managing firewall protection" on page 413.
Intrusion Prevention policy	The **Intrusion Prevention policy** automatically detects and blocks network attacks and attacks on browsers. **Note:** Intrusion Prevention policies can be applied only to Windows clients. See "Managing intrusion prevention on your client computers" on page 461.
LiveUpdate policy	The **LiveUpdate Content policy** and the **LiveUpdate Settings policy** contain the settings that determine how and when client computers download content updates from LiveUpdate. You can define the computers that clients contact to check for updates and schedule when and how often client computers check for updates. See "Managing content updates" on page 546.
Application and Device Control	The **Application and Device Control policy** protects a system's resources from applications and manages the peripheral devices that can attach to computers. See "Setting up application and device control" on page 482. **Note:** Application and Device Control policies can be applied only to Windows clients.
Host Integrity	The **Host Integrity policy** provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure. You use this policy to verify that the clients that access your network run the antivirus software, patches, and other application criteria that you define. See "What you can do with Host Integrity policies" on page 812.

Table 15-2   Security policy types *(continued)*

Policy type	Description
Exceptions policy	The **Exceptions policy** provides the ability to exclude applications and processes from detection by the virus and spyware scans and by SONAR.
	You can also exclude applications from application control.
	See "Managing exceptions for Symantec Endpoint Protection" on page 528.

About shared and non-shared policies

Policies are either shared or non-shared. A policy is shared if you apply it to more than one group or location. If you create shared policies, you can easily edit and replace a policy in all groups and locations that use it. You can apply shared policies at the My Company group level or a lower group level and subgroups can inherit policies. You can have multiple shared policies.

If you need a specialized policy for a particular group or location, you create a policy that is unique. You assign this unique, non-shared policy to one specific group or location. You can only have one policy of each policy type per location.

For example, here are some possible scenarios:

■ A group of users in Finance needs to connect to an enterprise network by using different locations when at the office and for home. You may need to apply a different Firewall policy with its own set of rules and settings to each location for that one group.

■ You have remote users who typically use DSL and ISDN, for which they may need a VPN connection. You have other remote users who want to dial up when they connect to the enterprise network. However, the sales and marketing groups also want to use wireless connections. Each of these groups may need its own Firewall policy for the locations from which they connect to the enterprise network.

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

You typically add any policy that groups and locations share in the **Policies** page on the **Policies** tab. However, you add any policy that is not shared between groups

and that applies only to a specific location in the **Clients** page. If you decide to add a policy in the **Clients** page, you can add a new policy by using any of the following methods:

- Add a new policy.
  See "Adding a policy" on page 296.

- Copy an existing policy to base the new policy on.
  See "Copying and pasting a policy on the Policies page" on page 298.
  See "Copying and pasting a policy on the Clients page" on page 298.

- Import a policy that was previously exported from another site.
  See "Exporting and importing individual policies" on page 303.

See "Performing the tasks that are common to all policies" on page 290.

See "Converting a shared policy to a non-shared policy " on page 304.

Adding a policy

Symantec Endpoint Protection Manager comes with a default policy for each type of protection. If you need to customize a policy, you add one and edit it. You can create multiple versions of each type of policy.

Symantec recommends that you test all new policies before you use them in a production environment.

To add a new policy

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

2 On the **Policies** page, select a policy type, and then click the link to add a new policy.

3 Modify the policy settings to increase or decrease protection.

4 Click **OK** to save the policy.

5 Optionally assign the new policy to a group.

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

   See "Assigning a policy to a group" on page 300.

See "Testing a policy" on page 301.

See "Performing the tasks that are common to all policies" on page 290.

Editing a policy

You can edit shared and non-shared policies on the **Policies** tab on the **Clients** page as well as on the **Policies** page.

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

See "Performing the tasks that are common to all policies" on page 290.

To edit a policy in the Policies page

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

2   On the **Policies** page, under **Policies**, click the policy type.

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

4   Under **Tasks**, click **Edit the Policy**.

5   In the *policy type* **Policy Overview** pane, edit the name and description of the policy, if necessary.

6   To edit the policy, click any of the *policy type* **Policy** pages for the policies.

To edit a policy in the Clients page

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

2   On the **Clients** page, under **Clients**, select the group for which you want to edit a policy.

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

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

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

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

6   To the right of the selected policy, click **Tasks**, and then click **Edit Policy**.

7   Do one of the following tasks:

   ■   To edit a non-shared policy, go to step 8.

   ■   To edit a shared policy, in the **Edit Policy** dialog box, click **Edit Shared** to edit the policy in all locations.

8   You can click a link for the type of policy that you want to edit.

Copying and pasting a policy on the Policies page

You can copy and paste a policy on the **Policies** page. For example, you may want to edit the policy settings slightly to apply to another group.

See "Performing the tasks that are common to all policies" on page 290.

To copy a policy in the Policies page

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

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

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

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

5   In the **Copy Policy** dialog box, check **Do not show this message again** if you no longer want to be notified about this process. The message states that the policy has been copied to the clipboard and is ready to be pasted.

6   Click **OK**.

To paste a policy in the Policies page

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

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

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

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

Copying and pasting a policy on the Clients page

You can copy and paste a policy instead of having to add a new policy. You can copy a shared or a non-shared policy on the **Clients** page.

See "Performing the tasks that are common to all policies" on page 290.

To copy a policy in the Clients page

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

2   On the **Clients** page, under **Clients**, select the group for which you want to copy a policy.

3   On the **Policies** tab, under **Location-specific Policies and Settings**, scroll to find the name of the location from which you want to copy a policy.

4 Locate the specific policy for the location that you want to copy.

5 To the right of the policy, click **Tasks**, and then click **Copy**.

6 Click **OK**.

To paste a policy on the Clients page

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

2 On the **Clients** page, under **Clients**, select the group for which you want to paste a policy.

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

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

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

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

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

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

Locking and unlocking Virus and Spyware policy settings

You can lock and unlock some Virus and Spyware Protection policy settings. End users cannot change locked settings. A padlock icon appears next to a lockable setting.

See "About access to the client interface" on page 237.

See "Performing the tasks that are common to all policies" on page 290.

To lock or unlock a policy setting

1 In the console, open a Virus and Spyware Protection policy.

2 Select one of the pages, such as **Auto-Protect.**

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

4 Click **OK**.

You can also lock and unlock Tamper Protection settings, Submissions settings, and intrusion prevention settings.

See "Changing Tamper Protection settings" on page 412.

See "Enabling or disabling client submissions to Symantec Security Response" on page 359.

See "Enabling or disabling network intrusion prevention or browser intrusion prevention" on page 467.

Assigning a policy to a group

You assign a policy to a client computer through a group. Every group has exactly one policy of each protection type that is assigned to it at all times. If you have both Windows clients and Mac clients, you can put them into separate groups or you can manage them in the same group. If you put them in the same group and apply a policy, each type of client applies the appropriate policy settings. Window computers ignore the settings that only apply to Mac computers, and Mac computers ignore the settings that only apply to Window computers.

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.

Policies are assigned to computer groups as follows:

■ At initial installation, the Symantec default security policies are assigned to the **My Company** parent group.

■ The security policies in the **My Company** parent group are automatically assigned to each newly created child group.

■ You replace a policy in a group by assigning another policy of the same type. You can replace a policy that is assigned to the **My Company** parent group or to any child group.

New groups always inherit from their immediate parent group. If you create a hierarchy of sub-groups, each one inherits from its immediate parent, not from the top-level parent.

The user interface in the **Assign policy** dialog box conveys the following additional information:

A folder icon indicates a group.

A round icon indicates a location.

- On a group icon, a check mark in a green circle indicates that this policy is assigned to all of the locations in the group.

- On a location icon, a check mark in a green circle indicates that this policy is assigned to this location.

- Text that is grayed out means that the group or location inherits its policy from its parent group.

See "Performing the tasks that are common to all policies" on page 290.

To assign a policy to a group

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

2   On the **Policies** page, select a policy, and then click **Assign the policy**.

3   In the **Assign policy** dialog box, select the groups, and then click **Assign**.

4   Click **OK** to confirm.

Testing a policy

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

See "Performing the tasks that are common to all policies" on page 290.

To test a policy

1   Create a group to use for policy testing.

    See "Adding a group" on page 210.

2   Assign the test policy to the test group.

    See "Assigning a policy to a group" on page 300.

3   Identify three or four managed computers to use for policy testing.

    If necessary, install the client software on the computers. Install the computers as managed computers.

    See "About client deployment methods" on page 131.

    See "About managed and unmanaged clients" on page 146.

4   Move the test computers to the test group.

    See "Moving a client computer to another group" on page 219.

5   Verify that the test computers got the latest policy.

See "How the client computers get policy updates" on page 307.

See "Using the policy serial number to check client-server communication" on page 309.

6   Run the test computers to verify that they operate correctly.

Replacing a policy

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

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

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

See "Performing the tasks that are common to all policies" on page 290.

To replace a shared policy for all locations

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

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

3   In the *policy type* **Policies** pane, click the policy.

4   In the **Policies** page, under **Tasks**, click **Replace the Policy**.

5   In the **Replace *policy type* Policy** dialog box, in the **New *policy type* Policy** list box, select the shared policy that replaces the old one.

6   Select the groups and locations for which you want to replace the existing policy.

7   Click **Replace**.

8   When you are prompted to confirm the replacement of the policy for the groups and locations, click **Yes**.

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

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

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

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

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

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

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

6   In the **Replace Policy** dialog box, in the **New policy** list box, select the
    replacement policy.

7   Click **OK**.

Exporting and importing individual policies

You can export and import policies rather than recreating the policies. All the
settings that are associated with the policy are automatically exported.

You may need to export a policy for the following reasons:

■   You update the management server from an older release to a newer release.
    You want to update the new management server with the policies that you
    previously customized.

■   You want to export a policy for use at a different site.

You can export and import policies in the following ways:

■   You export and import each policy one at a time. Once you export a file, you
    import it and apply it to a group or only to a location. You can export a shared
    or non-shared policy for a specific location in the **Clients** page.

■   You export and import all policies by using the server properties file. The
    server properties file includes all policies, locations, and server settings.
    Symantec recommends that you use this method if you upgrade a legacy version
    of the management server to the current version of the management server.
    See "Exporting and importing server settings" on page 719.

See "Performing the tasks that are common to all policies" on page 290.

To export a single policy from the Policies page

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

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

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

4 In the **Policies** page, under **Tasks**, click **Export the Policy**.

5 In the **Export Policy** dialog box, locate the folder where you want to export the policy file to, and then click **Export**.

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

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

2 Under **Clients**, select the group for which you want to export a policy.

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

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

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

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

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

7 In the **Export Policy** dialog box, browse to the folder into which you want to export the policy.

8 In the **Export Policy** dialog box, click **Export**.

To import a single policy

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

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

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

4 On the **Policies** page, under **Tasks**, click **Import a** *policy type* **Policy**.

5 In the **Import Policy** dialog box, browse to the policy file that you want to import, and then click **Import**.

Converting a shared policy to a non-shared policy

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

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

See "About shared and non-shared policies" on page 295.

See "Copying and pasting a policy on the Policies page" on page 298.

To convert a shared policy to a non-shared policy

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

2   In the **Clients** page, under **Clients**, select the group for which you want to convert a policy.

3   In the pane that is associated with the group that you selected in the previous step, click **Policies**.

4   On the **Policies** tab, uncheck **Inherit policies and settings from parent group** *group_name*.

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

5   Under **Location-specific Policies and Settings**, scroll to find the name of the location and the specific policy that you want to convert.

6   Beside the specific policy, click **Tasks**, and then click **Convert to Non-shared Policy**.

7   In the **Overview** dialog box, edit the name and description of the policy.

8   Modify the other policy settings as desired.

9   Click **OK**.

See "Performing the tasks that are common to all policies" on page 290.

Withdrawing a policy from a group

You may want to withdraw a policy from a group or a location under certain circumstances.

For example, a specific group may have experienced problems after you introduced a new policy. If you want the policy to remain in the database, you can withdraw the policy instead of deleting it. If you withdraw a policy, it is automatically withdrawn from the groups and locations that you assigned it to. The number of locations that a policy is used for appears on the *policy type* **Policies** pane on the **Policies** page.

Note: You must withdraw a policy or replace a policy from all groups and locations before you can delete it.

You can withdraw all policies in the **Policies** page from a location or group except for the following policies:

■ **Virus and Spyware Protection**

■ **LiveUpdate Settings**

You can only replace them with another **Virus and Spyware Protection policy** or **LiveUpdate policy**.

See "Replacing a policy" on page 302.

See "Assigning a policy to a group" on page 300.

To withdraw a shared policy in the Policies page

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

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

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

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

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

6   Click **Withdraw**.

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

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

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

2   On the **Clients** page, under **Clients**, select the group for which you want to withdraw a policy.

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

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

4   Under **Location-specific Policies and Settings**, scroll to find the name of the location for which you want to withdraw a policy.

5   Locate the policy for the location that you want to withdraw.

6 Click **Tasks**, and then click **Withdraw Policy**.

7 In the **Withdraw Policy** dialog box, click **Yes**.

See "Performing the tasks that are common to all policies" on page 290.

How the client computers get policy updates

When you configure policies on the management server, you need to have the updated policies downloaded to the client computers. In the console, you can configure client computers to use either of the following update methods:

Pull mode   The client computer connects to the management server periodically, depending on the frequency of the heartbeat setting. The client computer checks the status of the management server when the client connects.

Push mode   The client computer establishes a constant HTTP connection to the management server. Whenever a change occurs in the management server status, it notifies the client computer immediately.

In either mode, the client computer takes the corresponding action, based on the change in the status of the management server. Because it requires a constant connection, push mode requires a large amount of network bandwidth. Client computers that are configured to use pull mode require less bandwidth.

See "Configuring push mode or pull mode to update client policies and content" on page 308.

The heartbeat protocol defines the frequency at which client computers upload data such as log entries and download policies. The first heartbeat occurs immediately after the client starts. The next heartbeat occurs at the heartbeat frequency that you set.

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

Note: You can also update polices manually on a client computer.

See "Using the policy serial number to check client-server communication"
on page 309.

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

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

See "How the client computers get policy updates" on page 307.

See "Performing the tasks that are common to all policies" on page 290.

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

Note: If you installed Symantec Endpoint Protection Manager on a Windows XP
server, note that Windows XP supports a limited number of concurrent users if
the clients are in push mode. It is a best practice to use pull mode when you deploy
policies to up to 100 clients.

To configure push mode or pull mode for a group

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

2   Under **Clients**, select the group for which you want to specify whether to
    push or pull policies.

3   Click **Policies**.

4   Uncheck **Inherit policies and setting from the parent group "*group name*"**.

5   Under **Location-independent Policies and Settings** pane, under **Settings**,
    click **Communications Settings**.

6   In the **Communications Settings for *group name*** dialog box, under **Download**,
    verify that **Download policies and content from the management server** is
    checked.

7   Do one of the following tasks:

    ■ Click **Push mode**.

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

8   Click **OK**.

To specify push mode or pull mode for a location

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

2   Under **Clients**, select the group for which you want to specify whether to push or pull policies.

3   Click **Policies**.

4   Uncheck **Inherit policies and setting from the parent group "***group name***"**.

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

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

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

8   Do one of the following tasks:

- ■ Click **Push mode**.

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

9   Click **OK**.

See "Performing the tasks that are common to all policies" on page 290.

Using the policy serial number to check client-server communication

To check whether the server and client communicate, check the policy serial number on the console and on the client. If the client communicates with the management server and receives regular policy updates, the serial numbers should match.

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

See "Manually updating policies on the client" on page 310.

See "How the client computers get policy updates" on page 307.

To view the policy serial number in the console

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

2 Under **Clients**, select the relevant group.

The policy serial number and policy date appear in the upper right corner of the program window.

Note: The policy serial number and the policy date also appear at the bottom of the details list on the **Details** tab.

To view the policy serial number on the client computer

◆ On the client computer, in the client, click **Help > Troubleshooting**.

On the **Management** tab, look at the policy serial number.

The serial number should match the serial number on the console for the group that the client computer is in.

See "Performing the tasks that are common to all policies" on page 290.

Manually updating policies on the client

You can manually update the policies on the client computer if you do not think you have the latest policy on the client. If the client does not receive the update, there might be a communication problem.

Check the policy serial number to check whether your managed client computers can communicate with the management server.

See "Using the policy serial number to check client-server communication" on page 309.

To manually update policies from the client computer

1 On the client computer, in the client user interface, click **Help > Troubleshooting**.

2 In the **Troubleshooting** dialog box, in the left column, click **Management**.

3 On the **Management** panel, under **Policy Profile**, click **Update**.

To manually update policies from the console

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

2   Under **Clients**, right-click a group that is configured for pull mode, and then click **Run Command on Group**.

    Client computers that are configured for Push mode receive policy updates immediately, so you do not need to update them manually.

3   Click **Update Content**.

4   Check the policy serial numbers on the console and on a client computer to see if the numbers match.

See "Performing the tasks that are common to all policies" on page 290.

Monitoring the applications and services that run on client computers

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

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

■   Firewall policies

■   Application and Device Control policies

■   SONAR technology
    For legacy clients, TruScan proactive threat scans

■   Host Integrity policies

■   Network application monitoring

■   File fingerprint lists

Note: The Mac client does not monitor the applications and the services that run on Mac computers.

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

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

Table 15-3   Steps to monitor the applications

Steps	Description
Enable learned applications	Configure the management server to collect information about the applications that the client computers run.
	See "Configuring the management server to collect information about the applications that the client computers run" on page 313.
Search for applications	You can use a query tool to search for the list of applications that the client computers run. You can search on application-based criteria or computer-based criteria. For example, you can find out the version of Internet Explorer that each client computer uses.
	See "Searching for information about the applications that the computers run" on page 314.
	You can save the results of an application search for review.

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

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

You can enable learned applications for a group or a location. The clients then keep track of every application that runs and send that data to the management server.

Note: The Mac client does not monitor the applications and the services that run on Mac computers.

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

See "Setting up administrator notifications" on page 642.

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

To send the learned applications list to the management server for a group

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

2   Under **View Clients**, select a group.

3   On the **Policies** tab, click **Communications Settings**.

4   In the **Communications Settings for** *group name* dialog box, make sure **Learn applications that run on the client computers** is checked.

5   Click **OK**.

To send learned applications to the management server for a location

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

2   Under **View Clients**, select a group.

3   Under **Location-specific Policies and Settings**, select the location, and then expand **Location-specific Settings**.

4   To the right of **Communications Settings**, click **Tasks**, and then uncheck **Use Group Communications Settings**.

    Checking this setting enables you to create a location setting rather than a group setting.

5   Click **Tasks**, and then click **Edit Settings**.

6 In the **Communications Settings for** *location name* dialog box, check **Learn applications that run on the client computers**.

7 Click **OK**.

See "Monitoring the applications and services that run on client computers" on page 311.

See "Performing the tasks that are common to all policies" on page 290.

Searching for information about the applications that the computers run

After the management server receives the list of applications from the clients, you can run queries to find out details about the applications. For example, you can find all the client computers that use an unauthorized application. You can then create a firewall rule to block the application on the client computer. Or you may want to upgrade all the client computers to use the most current version of Microsoft Word. You can use the **Search for Applications** task from any type of policy.

Note: The Mac client does not monitor the applications and the services that run on Mac computers.

You can search for an application in the following ways:

■ By application.
  You can limit the search to specific applications or application details such as its name, file fingerprint, path, size, version, or last modified time.

■ By client or client computer.
  You can search for the applications that either a specific user runs or a specific computer runs. For example, you can search on the computer's IP address.

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

See "Defining information about applications" on page 436.

Note: The information in the **Search** box is not collected until you enable the feature that keeps track of all the applications that clients run. You can go to the **Clients** page, **Communications Settings** dialog box for each group or location to enable this feature.

To search for information about the applications that the computers run

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

2   On the **Policies** page, under **Tasks**, click **Search for Applications**.

3   In the **Search for Applications** dialog box, to the right of the **Search for applications in** field, click **Browse**.

4   In the **Select Group or Location** dialog box, select a group of clients for which you want to view the applications, and then click **OK**.

    You can specify only one group at a time.

5   Make sure that **Search subgroups** is checked.

6   Do one of the following actions:

    ■   To search by user or computer information, click **Based on client/computer information**.

    ■   To search by application, click **Based on applications**.

7   Click the empty cell under **Search Field**, and then select the search criterion from the list.

    The Search Field cell displays the criteria for the option that you selected. For details about these criteria, click **Help**.

8   Click the empty cell under Comparison Operator, and then select one of the operators.

9   Click the empty cell under Value, and then select or type a value.

    The Value cell may provide a format or a value from the drop-down list, depending on the criterion you selected in the Search Field cell.

10 To add an additional search criterion, click the second row, and then enter information in the Search Field, Comparison Operator, and Value cells.

    If you enter more than one row of search criteria, the query tries to match all conditions.

11 Click **Search**.

12 In the Query Results table, do any of the following tasks:

    ■   Click the scroll arrows to view additional rows and columns.

    ■   Click **Previous** and **Next** to see additional screens of information.

    ■   Select a row, and then click **View Details** to see additional information about the application.

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

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

14 Click **Close**.

See "Monitoring the applications and services that run on client computers" on page 311.

See "Performing the tasks that are common to all policies" on page 290.

Chapter 16

Managing Virus and Spyware Protection

This chapter includes the following topics:

- Preventing and handling virus and spyware attacks on client computers

- Remediating risks on the computers in your network

- Managing scans on client computers

- Setting up scheduled scans that run on Windows computers

- Setting up scheduled scans that run on Mac computers

- Running on-demand scans on client computers

- Adjusting scans to improve computer performance

- Adjusting scans to increase protection on your client computers

- Managing Download Insight detections

- How Symantec Endpoint Protection uses reputation data to make decisions about files

- How Symantec Endpoint Protection policy features work together

- About submitting information about detections to Symantec Security Response

- About submissions throttling

- Enabling or disabling client submissions to Symantec Security Response

- Specifying a proxy server for client submissions and other external communications

- Managing the Quarantine

- Managing the virus and spyware notifications that appear on client computers

- About the pop-up notifications that appear on the clients that run Windows 8

- Enabling or disabling Symantec Endpoint Protection pop-up notifications on Windows 8 clients

- Managing early launch anti-malware (ELAM) detections

- Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options

Preventing and handling virus and spyware attacks on client computers

You can prevent and handle virus and spyware attacks on client computers by following some important guidelines.

Table 16-1   Protecting computers from virus and spyware attacks

Task	Description
Make sure that your computers have Symantec Endpoint Protection installed	All computers in your network and all your servers should have Symantec Endpoint Protection installed. Make sure that Symantec Endpoint Protection is functioning correctly.
Keep definitions current	Make sure that the latest definitions are installed on client computers.
	You can check the definitions date on the **Clients** tab. You can run a command to update the definitions that are out of date.
	You can also run a computer status report to check the latest definitions date.
	See "Managing content updates" on page 546.

Table 16-1   Protecting computers from virus and spyware attacks *(continued)*

Task	Description
Run regular scans	By default, Auto-Protect and SONAR run on client computers. A default scheduled active scan also runs on client computers.
	You can run scans on demand. You can customize the scan settings.
	See "Running on-demand scans on client computers" on page 344.
	You might want to create and customize scheduled scans.
	Typically, you might want to create a full scheduled scan to run once a week, and an active scan to run once per day. By default, Symantec Endpoint Protection generates an active scan that runs at 12:30 P.M. On unmanaged computers, Symantec Endpoint Protection also includes a default startup scan that is disabled.
	You should make sure that you run an active scan every day on the computers in your network. You might want to schedule a full scan once a week or once a month if you suspect that you have an inactive threat in your network. Full scans consume more computer resources and might affect computer performance.
	See "Setting up scheduled scans that run on Windows computers" on page 341.
	See "Setting up scheduled scans that run on Mac computers" on page 344.
Check or modify scan settings for increased protection	By default, virus and spyware scans detect, remove, and repair the side effects of viruses and security risks.
	The default scan settings optimize your client computers' performance while still providing a high level of protection. You can increase the level of protection, however.
	For example, you might want to increase the Bloodhound™ heuristic protection.
	You also might want to enable scans of network drives.
	See "Adjusting scans to increase protection on your client computers" on page 348.
Allow clients to submit information about detections to Symantec	Clients can submit information about detections to Symantec. The submitted information helps Symantec address threats.
	See "Enabling or disabling client submissions to Symantec Security Response" on page 359.
Run intrusion prevention	Symantec recommends that you run intrusion prevention on your client computers as well as Virus and Spyware Protection.
	See "Managing intrusion prevention on your client computers" on page 461.

Table 16-1	Protecting computers from virus and spyware attacks *(continued)*

Task	Description
Remediate infections if necessary	After scans run, client computers might still have infections. For example, a new threat might not have a signature, or Symantec Endpoint Protection was not able to completely remove the threat. In some cases client computers require a restart for Symantec Endpoint Protection to complete the cleaning process. See "Remediating risks on the computers in your network" on page 320.

Remediating risks on the computers in your network

You remediate risks as part of handling virus and spyware attacks on your computers.

You use the Reports and Monitors features in the console to determine what computers are infected and to view the results of remediation.

Table 16-2	Remediating risks on client computers

Step	Task	Description
Step 1	Identify infected and at-risk computers	You can get information about infected and at-risk computers from Symantec Endpoint Protection Manager. On the Home page, check the Newly Infected and the Still Infected counts in the Virus and Risks Activity Summary. The Newly Infected count is a subset of the Still Infected count. The Newly Infected count shows the number of infected and at-risk computers during the time interval that you specify in the summary. **Note:** Unremediated SONAR detections are not counted as Still Infected. They are part of the Suspicious count in the summary. Computers are considered still infected if a subsequent scan detects them as infected. For example, a scheduled scan might partially clean a file. Auto-Protect subsequently detects the file as a risk. Files that are considered "still infected" are rescanned when new definitions arrive or as soon as the client computer is idle. See "Identifying the infected and at-risk computers" on page 322.

Table 16-2   Remediating risks on client computers *(continued)*

Step	Task	Description
Step 2	Update definitions and rescan	You should make sure that clients use the latest definitions.
		For the clients that run on Windows computers, you should also make sure that your scheduled and on-demand scans use the Insight Lookup feature.
		You can check the definitions date in the Infected and At Risk Computers report. You can run the Update Content and Scan command from the Risk log.
		When the Virus and Risks Activity Summary on the Home page shows the Still Infected and the Newly Infected counts are zero, then all risks are eliminated.
		See "Managing content updates" on page 546.
Step 3	Check scan actions and rescan	Scans might be configured to leave the risk alone. You might want to edit the Virus and Spyware Protection policy and change the action for the risk category. The next time the scan runs, Symantec Endpoint Protection applies the new action.
		You set the action on the **Actions** tab for the particular scan type (administrator-defined or on-demand scan, or Auto-Protect). You can also change the detection action for Download Insight and SONAR.
		See "Checking the scan action and rescanning the identified computers" on page 322.
Step 4	Restart computers if necessary to complete remediation	Computers may still be at risk or infected because they need to be restarted to finish the remediation of a virus or security risk.
		You can view the Risk log to determine if any computers require a restart.
		You can run a command from the logs to restart computers.
		See "Running commands from the computer status log" on page 630.
Step 5	Investigate and clean remaining risks	If any risks remain, you should to investigate them further.
		You can check the Symantec Security Response Web page for up-to-date information about viruses and security risks.
		http://securityresponse.symantec.com
		On the client computer, you can also access the Security Response Web site from the scan results dialog box.
		Symantec Technical Support also offers a Threat Expert tool that quickly provides detailed analysis of threats. You can also run a loadpoint analysis tool that can help you troubleshoot problems.
Step 6	Check the Computer Status log	View the Computer Status log to make sure that risks are remediated or removed from client computers.
		See "Viewing logs" on page 624.

For more information about handling viruses and outbreaks on a network, see the knowledge base article, Best practices for troubleshooting viruses on a network.

See "Preventing and handling virus and spyware attacks on client computers" on page 318.

See "Monitoring endpoint protection" on page 603.

Identifying the infected and at-risk computers

You can use the Symantec Endpoint Protection Manager Home page and a Risk report to identify the computers that are infected and at risk.

To identify infected computers

1   In the console, click **Home** and view the Virus and Risks Activity Summary.

   If you are a system administrator, you see counts of the number of Newly Infected and Still infected computers in your site. If you are a domain administrator, you see counts of the number of Newly Infected and Still infected computers in your domain.

   Still Infected is a subset of Newly Infected, and the Still Infected count goes down as you eliminate the risks from your network. Computers are still infected if a subsequent scan would report them as infected. For example, Symantec Endpoint Protection might have been able to clean a risk only partially from a computer, so Auto-Protect still detects the risk.

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

3   In the **Report type** list box, click **Risk**.

4   In the **Select a report** list box, click **Infected and At Risk Computers**.

5   Click **Create Report** and note the lists of the infected and at-risk computers that appear.

See "Remediating risks on the computers in your network" on page 320.

Checking the scan action and rescanning the identified computers

If you have infected and at-risk computers, you should identify why the computers are still infected or at risk. Check the action that was taken for each risk on the infected and at risk computers. It may be that the action that was configured and taken was Left Alone. If the action was Left Alone, you should either clean the risk from the computer, remove the computer from the network, or accept the risk. For Windows clients, you might want to edit the Virus and Spyware Protection policy and change the scan action.

See "Remediating risks on the computers in your network" on page 320.

To identify the actions that need to be changed and rescan the identified computers

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

2 On the **Logs** tab, select the Risk log, and then click **View Log**.

   From the Risk log event column, you can see what happened and the action that was taken. From the Risk Name column, you can see the names of the risks that are still active. From the Domain Group User column you can see which group the computer is a member of.

   If a client is at risk because a scan took the action **Left Alone**, you may need to change the Virus and Spyware Protection policy for the group. In the **Computer** column, you can see the names of the computers that still have active risks on them.

   See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 389.

   If your policy is configured to use Push mode, it is pushed out to the clients in the group at the next heartbeat.

   See "How the client computers get policy updates" on page 307.

3 Click **Back**.

4 On the **Logs** tab, select the Computer Status log, and then click **View Log**.

5 If you changed an action and pushed out a new policy, select the computers that need to be rescanned with the new settings.

6 In the **Command** list box, select **Scan**, and then click **Start** to rescan the computers.

   You can monitor the status of the Scan command from the **Command Status** tab.

Managing scans on client computers

Some scans run by default, but you might want to change settings or set up your own scheduled scans. You can also customize scans and change how much protection they provide on your client computers.

Table 16-3 Managing scans on client computers

Task	Description
Review the types of scans and default settings	Check your scan settings. You can review the defaults and determine if you want to make changes. See "About the types of scans and real-time protection" on page 326. See "About the default Virus and Spyware Protection policy scan settings" on page 336.
Create scheduled scans and run on-demand scans	You use scheduled scans and on-demand scans to supplement the protection that Auto-Protect provides. Auto-Protect provides protection when you read and write files. Scheduled scans and on-demand scans can scan any files that exist on your client computers. They can also protect memory, load points, and other important locations on your client computers. **Note:** For managed clients, Symantec Endpoint Protection provides a default scheduled scan that scans all files, folders, and locations on the client computers. See "Setting up scheduled scans that run on Windows computers" on page 341. See "Setting up scheduled scans that run on Mac computers" on page 344. See "Running on-demand scans on client computers" on page 344.
Customize scan settings for your environment	You can customize Auto-Protect settings as well as options in administrator-defined scans. You might want to change scan settings to handle false positive detections, optimize computer or scan performance, or change scan actions or notifications. For scheduled scans, you can also set options for missed scans, randomized scans, and whether or not to scan network drives. See "Customizing the virus and spyware scans that run on Windows computers" on page 376. See "Customizing the virus and spyware scans that run on Mac computers" on page 377.
Adjust scans to improve client computer performance	By default, Symantec Endpoint Protection provides a high level of security while it minimizes the effect on your client computers' performance. You can change some settings, however, to optimize the computer performance even more. Optimization is important in virtualized environments. **Note:** When you adjust settings to optimize client computer performance, you might decrease some security on your client computers. See "Adjusting scans to improve computer performance" on page 346.

Table 16-3   Managing scans on client computers *(continued)*

Task	Description
Adjust scans to increase protection on your client computers	The default scan settings optimize your client computers' performance while still providing a high level of protection. You can increase the level of protection, however. See "Adjusting scans to increase protection on your client computers" on page 348.
Manage Download Insight detections	Download Insight inspects files that users try to download through Web browsers, text messaging clients, and other portals. Download Insight uses reputation information from Symantec Insight to make decisions about files. See "Managing Download Insight detections" on page 351.
Manage SONAR	SONAR is part of Proactive Threat Protection on your client computers. However, SONAR settings are part of a Virus and Spyware Protection policy. See "Managing SONAR" on page 397.
Configure exceptions for scans	You can create exceptions for the files and applications that you know are safe. Symantec Endpoint Protection also excludes some files and folders automatically. See "Managing exceptions for Symantec Endpoint Protection" on page 528. See "About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans" on page 332.
Manage files in the Quarantine	You can monitor and delete the files that are quarantined on your client computers. You can also specify settings for the Quarantine. See "Managing the Quarantine" on page 363.
Allow clients to submit information about detections to Symantec	By default, clients send information about detections to Symantec. You can turn off submissions or choose which types of the information that clients submit. Symantec recommends that you always allow clients to send submissions. The information helps Symantec address threats. See "Enabling or disabling client submissions to Symantec Security Response" on page 359.
Manage the virus and spyware notifications that appear on client computers	You can decide whether or not notifications appear on client computers for virus and spyware events. See "Managing the virus and spyware notifications that appear on client computers" on page 368.

About the types of scans and real-time protection

Symantec Endpoint Protection includes different types of scans and real-time protection to detect different types of viruses, threats, and risks.

By default, Symantec Endpoint Protection runs an active scan every day at 12:30 P.M. Symantec Endpoint Protection also runs an active scan when new definitions arrive on the client computer. On unmanaged computers, Symantec Endpoint Protection also includes a default startup scan that is disabled.

Note: When a client computer is off or in hibernation or sleep mode, the computer might miss a scheduled scan. When the computer starts up or wakes, by default the scan is retried within a specified interval. If the interval already expired, Symantec Endpoint Protection does not run the scan and waits until the next scheduled scan time. You can modify the settings for missed scheduled scans.

You should make sure that you run an active scan every day on the computers in your network. You might want to schedule a full scan once a week or once a month if you suspect that you have an inactive threat in your network. Full scans consume more computer resources and might affect computer performance.

See "Managing scans on client computers" on page 323.

Table 16-4   Scan types

Scan type	Description
Auto-Protect	Auto-Protect continuously inspects files and email data as they are written to or read from a computer. Auto-Protect automatically neutralizes or eliminates detected viruses and security risks.
	Note: Mac clients support Auto-Protect for the file system only.
	See "About the types of Auto-Protect" on page 328.
Download Insight	Download Insight boosts the security of Auto-Protect scans by inspecting files when users try to download them from browsers and other portals. It uses reputation information from Symantec Insight to allow or block download attempts.
	Download Insight functions as part of Auto-Protect and requires Auto-Protect to be enabled.
	See "How Symantec Endpoint Protection uses reputation data to make decisions about files" on page 355.

Table 16-4   Scan types *(continued)*

Scan type	Description
Administrator-defined scans	Administrator-defined scans detect viruses and security risks by examining all files and processes on the client computer. Administrator-defined scans can also inspect memory and load points.
	The following types of administrator-defined scans are available:
	■ Scheduled scans A scheduled scan runs on the client computers at designated times. Any concurrently scheduled scans run sequentially. If a computer is turned off or in hibernation or sleep mode during a scheduled scan, the scan does not run unless it is configured to retry missed scans. When the computer starts or wakes, Symantec Endpoint Protection retries the scan until the scan starts or the retry interval expires. You can schedule an active, full, or custom scan.
	Note: Only custom scans are available for Mac clients.
	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 scan. The scan templates can save you time when you configure multiple policies. A scheduled scan template is included by default in the policy. The default scheduled scan scans all files and directories.
	■ Startup scans and triggered scans Startup scans run when the users log on to the computers. Triggered scans run when new virus definitions are downloaded to computers.
	Note: Startup scans and triggered scans are available only for Windows clients.
	■ On-demand scans On-demand scans are the scans that run immediately when you select the scan command in Symantec Endpoint Protection Manager. You can select the command from the Clients tab or from the logs.
SONAR	SONAR offers real-time protection against zero-day attacks. SONAR can stop attacks even before traditional signature-based definitions detect a threat. SONAR uses heuristics as well as file reputation data to make decisions about applications or files.
	Like proactive threat scans, SONAR detects keyloggers, spyware, and any other application that might be malicious or potentially malicious.
	Note: SONAR is only supported on Windows computers that run Symantec Endpoint Protection version 12.1 and later.
	See "About SONAR" on page 395.

| | **Table 16-4** | Scan types *(continued)* |

Scan type	Description
TruScan proactive threat scans	Supported on Windows computers that run Symantec Endpoint Protection version 11.x. SONAR is not supported on any computers that run version 11.x.
	TruScan proactive threat scans provide protection to legacy clients against zero-day attacks. TruScan proactive threat scans determine if an application or a process exhibits characteristics of known threats. These scans detect Trojan horses, worms, keyloggers, adware and spyware, and the applications that are used for malicious purposes.
	Unlike SONAR, which runs in real time, TruScan proactive threat scans run on a set frequency.
Early launch anti-malware (ELAM)	Works with the Windows early launch anti-malware driver. Supported only on Windows 8.
	Early launch anti-malware provides protection for the computers in your network when they start up and before third-party drivers initialize.
	See "Managing early launch anti-malware (ELAM) detections" on page 371.

About the types of Auto-Protect

Auto-Protect scans files as well as certain types of email and email attachments.

By default, all types of Auto-Protect are enabled. If your client computers run other email security products, such as Symantec Mail Security, you might not need to enable Auto-Protect for email.

Mac clients do not support Auto-Protect scans of email.

See "About the types of scans and real-time protection" on page 326.

Table 16-5   Types of Auto-Protect

Type of Auto-Protect	Description
Auto-Protect	Continuously scans files as they are read from or written to the client computer.
	Auto-Protect is enabled by default for the file system. It loads at computer startup. It inspects all files for viruses and security risks, and blocks the security risks from being installed. It can optionally scan files by file extension, scan files on remote computers, and scan floppies for boot viruses. It can optionally back up files before it attempts to repair the files, and terminate processes and stop services.
	You can configure Auto-Protect to scan only selected file extensions. When Auto-Protect scans the selected extensions, it can also determine a file's type even if a virus changes the file's extension.
	For Mac clients or Windows clients that do not run email Auto-Protect, your client computers are still protected when Auto-Protect is enabled. Most email applications save attachments to a temporary folder when users launch email attachments. Auto-Protect scans the file as it is written to the temporary folder and detects any virus or security risk. Auto-Protect also detects the virus if the user tries to save an infected attachment to a local drive or network drive.
Internet Email Auto-Protect	Scans Internet email (POP3 or SMTP) and attachments for viruses and security risks; also performs outbound email heuristics scanning.
	By default, Internet Email Auto-Protect supports encrypted passwords and email over POP3 and SMTP connections. If you use POP3 or SMTP with Secure Sockets Layer (SSL), then the client detects secure connections but does not scan encrypted messages.
	Note: For performance reasons, Internet Email Auto-Protect for POP3 is not supported on server operating systems. Internet email scanning is not supported for 64-bit computers.
	Email scanning does not support IMAP, AOL, or HTTP-based email such as Hotmail or Yahoo! Mail.

Table 16-5	Types of Auto-Protect *(continued)*
Type of Auto-Protect	**Description**
Microsoft Outlook Auto-Protect	Scans Microsoft Outlook email (MAPI and Internet) and attachments for viruses and security risks. Supported for Microsoft Outlook 98/2000/2002/2003/2007/2010 (MAPI and Internet). If Microsoft Outlook is already installed on the computer when you perform a client software installation, the client software detects the email application. The client automatically installs Microsoft Outlook Auto-Protect. If you use Microsoft Outlook over MAPI or Microsoft Exchange client and you have Auto-Protect enabled for email, attachments are scanned when the user opens the attachment. If a user downloads a large attachment over a slow connection, mail performance is affected. You may want to disable this feature for users who regularly receive large attachments. **Note:** On a Microsoft Exchange Server, you should not install Microsoft Outlook Auto-Protect. Instead you should install Symantec Mail Security for Microsoft Exchange.
Lotus Notes Auto-Protect	Scans Lotus Notes email and attachments for viruses and security risks. Supported for Lotus Notes 7.x or later. If Lotus Notes is already installed on the computer when you perform a client software installation, the client software detects the email application. The client automatically installs Lotus Notes Auto-Protect.

About virus and security risks

Symantec Endpoint Protection scans for both viruses and for security risks. Viruses and security risks can arrive through email messages or instant messenger programs. Often a user unknowingly downloads a risk by accepting an End User License Agreement from a software program.

Many viruses and security risks are installed as drive-by downloads. These downloads usually occur when users visit malicious or infected Web sites, and the application's downloader installs through a legitimate vulnerability on the computer.

On Windows clients, you can change the action that Symantec Endpoint Protection takes when it detects a virus or a security risk. The security risk categories are dynamic and change over time as Symantec collects information about risks.

See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 389.

You can view information about specific virus and security risks on the Symantec Security Response Web site.

Table 16-6   Viruses and security risks

Risk	Description
Viruses	Programs or code that attach a copy of themselves to another computer program or file when it runs. When the infected program runs, the attached virus program activates and attaches itself to other programs and files.
	The following types of threats are included in the virus category:
	■ Malicious Internet bots Programs that run automated tasks over the Internet. Bots can be used to automate attacks on computers or to collect information from Web sites. ■ Worms Programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate in memory to reduce computer performance. ■ Trojan horses Programs that hide themselves in something benign, such as a game or utility. ■ Blended threats Threats that blend the characteristics of viruses, worms, Trojan horses, and code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. Blended threats use multiple methods and techniques to spread rapidly and cause widespread damage. ■ Rootkits Programs that hide themselves from a computer's operating system.
Adware	Programs that deliver any advertising content.
Dialers	Programs that use a computer, without the user's permission or knowledge, to dial out through the Internet to a 900 number or FTP site. Typically, these numbers are dialed to accrue charges.

Table 16-6   Viruses and security risks *(continued)*

Risk	Description
Hacking tools	Programs that hackers use to gain unauthorized access to a user's computer. For example, one hacking tool is a keystroke logger, which tracks and records individual keystrokes and sends this information back to the hacker. The hacker can then perform port scans or vulnerability scans. Hacking tools may also be used to create viruses.
Joke programs	Programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or frightening. For example, a joke program might move the recycle bin away from the mouse when the user tries to delete an item.
Misleading applications	Applications that intentionally misrepresent the security status of a computer. These applications typically masquerade as security notifications about any fake infections that must be removed.
Parental control programs	Programs that monitor or limit computer usage. The programs can run undetected and typically transmit monitoring information to another computer.
Remote access programs	Programs that allow access over the Internet from another computer so that they can gain information or attack or alter a user's computer.
Security assessment tool	Programs that are used to gather information for unauthorized access to a computer.
Spyware	Stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and relay it back to another computer.
Trackware	Stand-alone or appended applications that trace a user's path on the Internet and send information to the controller or hacker's system.

About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans

When Symantec Endpoint Protection detects the presence of certain third-party applications and some Symantec products, it automatically creates exclusions for these files and folders. The client excludes these files and folders from all scans.

Note: The client does not exclude the system temporary folders from scans because doing so can create a significant security vulnerability on a computer.

To improve scan performance or reduce false positive detections, you can exclude files by adding a file or a folder exception to an Exceptions policy. You can also specify the file extensions or the folders that you want to include in a particular scan.

Warning: The files or folders that you exclude from scans are not protected from viruses and security risks.

You can view the exclusions that the client automatically creates.

Look in the following locations of the Windows registry:

■ On 32-bit computers, see HKEY_LOCAL_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\Exclusions.

■ On 64-bit computers, see HKEY_LOCAL_MACHINE\Software\Wow6432Node\Symantec\Symantec Endpoint Protection\AV\Exclusions.

Warning: Do not edit this registry directly.

Table 16-7	File and folder exclusions

Files	Description
Microsoft Exchange	The client software automatically creates file and folder scan exclusions for the following Microsoft Exchange Server versions: ■ Exchange 5.5 ■ Exchange 6.0 ■ Exchange 2000 ■ Exchange 2003 ■ Exchange 2007 ■ Exchange 2007 SP1 ■ Exchange 2010 For Exchange 2007, see your user documentation for information about compatibility with antivirus software. In a few circumstances, you might need to create scan exclusions for some Exchange 2007 folders manually. For example, in a clustered environment, you might need to create some exclusions. The client software checks for changes in the location of the appropriate Microsoft Exchange files and folders at regular intervals. If you install Microsoft Exchange on a computer where the client software is already installed, the exclusions are created when the client checks for changes. The client excludes both files and folders; if a single file is moved from an excluded folder, the file remains excluded. For more information, see the knowledge base article, Preventing Symantec Endpoint Protection from scanning the Microsoft Exchange 2007 directory structure.
Microsoft Forefront	The client automatically creates file and folder exclusions for the following Microsoft Forefront products: ■ Forefront Server Security for Exchange ■ Forefront Server Security for SharePoint ■ Forefront Threat Management Gateway Check the Microsoft Web site for a list of recommended exclusions. Also see the Symantec Technical Support knowledge base article, Configuring Symantec Endpoint Protection exclusions for Microsoft Forefront.
Active Directory domain controller	The client automatically creates file and folder exclusions for the Active Directory domain controller database, logs, and working files. The client monitors the applications that are installed on the client computer. If the software detects Active Directory on the client computer, the software automatically creates the exclusions.

Table 16-7   File and folder exclusions *(continued)*

Files	Description
Symantec products	The client automatically creates appropriate file and folder scan exclusions for certain Symantec products when they are detected.
	The client creates exclusions for the following Symantec products:
	■ Symantec Mail Security 4.0, 4.5, 4.6, 5.0, and 6.0 for Microsoft Exchange
	■ Symantec AntiVirus/Filtering 3.0 for Microsoft Exchange
	■ Norton AntiVirus 2.x for Microsoft Exchange
	■ Symantec Endpoint Protection Manager embedded database and logs
Selected extensions and Microsoft folders	For each type of administrator-defined scan or Auto-Protect, you can select files to include by extension. For administrator-defined scans, you can also select files to include by folder. For example, you can specify that a scheduled scan only scans certain extensions and that Auto-Protect scans all extensions.
	For executable files and Microsoft Office files, Auto-Protect can determine a file's type even if a virus changes the file's extension.
	By default Symantec Endpoint Protection scans all extensions and folders. Any extensions or folders that you deselect are excluded from that particular scan.
	Symantec does not recommend that you exclude any extensions from scans. If you decide to exclude files by extension and any Microsoft folders, however, you should consider the amount of protection that your network requires. You should also consider the amount of time and resources that your client computers require to complete the scans.
	Note: Any file extensions that you exclude from Auto-Protect scans of the file system also excludes the extensions from Download Insight. If you are running Download Insight, you should include extensions for common programs and documents in the list of extensions that you want to scan. You should also make sure that you scan .msi files.
File and folder exceptions	You use an Exceptions policy to create exceptions for the files or the folders that you want Symantec Endpoint Protection to exclude from all virus and spyware scans.
	Note: By default, users on client computers can also create file and folder exceptions.
	For example, you might want to create file exclusions for an email application inbox.
	If the client detects a virus in the Inbox file during an on-demand or scheduled scan, the client quarantines the entire inbox. You can create an exception to exclude the inbox file instead. If the client detects a virus when a user opens an email message, however, the client still quarantines or deletes the message.

Table 16-7   File and folder exclusions *(continued)*

Files	Description
Trusted files	Virus and spyware scans include a feature that is called Insight that lets scans skip trusted files. You can choose the level of trust for the files that you want to skip, or you can disable the option. If you disable the option, you might increase scan time. Auto-Protect can also skip the files that are accessed by trusted processes such as Windows Search.

See "Excluding a file or a folder from scans" on page 534.

About the default Virus and Spyware Protection policy scan settings

Symantec Endpoint Protection Manager includes three default policies.

- Virus and Spyware Protection Balanced policy

- Virus and Spyware Protection High Security policy
  The High Security policy is the most stringent of all the preconfigured policies. You should be aware that it can affect the performance of other applications.

- Virus and Spyware Protection High Performance policy
  The High Performance policy provides better performance than the High Security policy, but it does not provide the same safeguards. The policy relies primarily on Auto-Protect to scan files with selected file extensions to detect threats.

The basic Virus and Spyware Protection policy provides a good balance between security and performance.

Table 16-8   Virus and Spyware Protection Balanced policy scan settings

Setting	Description
Auto-Protect for the file system	Enabled Download Insight malicious file sensitivity is set to level 5. The Download Insight action for unproven files is **Ignore**. Auto-Protect includes the following settings: ■ Scans all files for viruses and security risks. ■ Blocks the security risks from being installed. ■ Cleans the virus-infected files. Backs up the files before it repairs them. Quarantines the files that cannot be cleaned. ■ Quarantines the files with security risks. Logs the files that cannot be quarantined. ■ Checks all floppies for boot viruses. Logs the boot viruses. ■ Notifies the computer users about viruses and security risks.
Auto-Protect for email	Enabled Other types of Auto-Protect include the following settings: ■ Scans all files, including the files that are inside compressed files. ■ Cleans the virus-infected files. Quarantines the files that cannot be cleaned. ■ Quarantines the files with security risks. Logs the files that cannot be quarantined. ■ Sends a message to the computer users about detected viruses and security risks.
SONAR	Enabled for Symantec Endpoint Protection 12.1 clients and later. Legacy clients use TruScan settings. TruScan is enabled when SONAR is enabled. High risk heuristic detections are quarantined Logs any low risk heuristic detections Aggressive mode is disabled **Show alert upon detection** is enabled System change detection actions are set to Ignore. Suspicious behavior detection blocks high risk threats and ignores low risk threats.

| Table 16-8 | Virus and Spyware Protection Balanced policy scan settings *(continued)* |

Setting	Description
Administrator-defined scans	The scheduled scan includes the following default settings: ■ Performs an active scan every day at 12:30 P.M. The scan is randomized. ■ Scans all files and folders, including the files that are contained in compressed files. ■ Scans memory, common infection locations, and known virus and security risk locations. ■ Cleans the virus-infected files. Backs up the files before it repairs them. Quarantines the files that cannot be cleaned. ■ Quarantines the files with security risks. Logs the files that cannot be quarantined. ■ Retries missed scans within three days. ■ Insight Lookup is set to level 5. The on-demand scan provides the following protection: ■ Scans all files and folders, including the files that are contained in compressed files. ■ Scans memory and common infection locations. ■ Cleans the virus-infected files. Backs up the files before it repairs them. Quarantines the files that cannot be cleaned. ■ Quarantines the files with security risks. Logs the files that cannot be quarantined.

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

| Table 16-9 | Virus and Spyware Protection High Security policy settings |

Setting	Description
Auto-Protect for the file system and email	Same as Virus and Spyware Protection Balanced policy Auto-Protect also inspects the files on the remote computers.
SONAR	Same as Virus and Spyware Protection Balanced policy but with the following changes: Blocks any system change events.
Global settings	Bloodhound is set to Aggressive.

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

Table 16-10   Virus and Spyware Protection High Performance policy settings

Setting	Description
Auto-Protect for the file system	Same as Virus and Spyware Protection Balanced policy but with the following changes: ■ Download Insight malicious file sensitivity is set to level 1.
Internet Email Auto-Protect Microsoft Outlook Auto-Protect Lotus Notes Auto-Protect	Disabled
SONAR	Same as Virus and Spyware Protection policy with the following changes: Ignores any system change events. Ignores any behavioral policy enforcement events.
Administrator-defined scans	Same as Virus and Spyware Protection policy except the following setting: ■ Insight Lookup is set to level 1.

How Symantec Endpoint Protection handles detections of viruses and security risks

Symantec Endpoint Protection uses default actions to handle the detection of viruses and security risks. You can change some of the defaults.

Table 16-11   How Symantec Endpoint Protection handles the detection of viruses and security risks

Detection	Description
Viruses	By default, the Symantec Endpoint Protection client first tries to clean a file that a virus infects.
	If the client software cannot clean the file, it does the following actions:
	■ Moves the file to the Quarantine on the infected computer ■ Denies any access to the file ■ Logs the event
Security risks	By default, the client moves any files that security risks infect to the Quarantine on the infected computer. The client also tries to remove or repair the risk's side effects.
	If a security risk cannot be quarantined and repaired, the second action is to log the risk.
	By default, the Quarantine contains a record of all actions that the client performed. You can return the client computer to the state that existed before the client tried the removal and repair.
	On Windows client computers, you can disable Auto-Protect scanning for security risks. You might want to temporarily disable Auto-Protect scanning of security risks if detection of a security risk could compromise a computer's stability. Scheduled and on-demand scans continue to detect the risk.

Detections by SONAR are considered suspicious events. You configure actions for these detections as part of the SONAR configuration.

See "Managing SONAR" on page 397.

For Windows client computers, you can assign a first and a second action for Symantec Endpoint Protection to take when it finds risks. You can configure different actions for viruses and security risks. You can use different actions for scheduled, on-demand, or Auto-Protect scans.

Note: On Windows client computers, the list of the detection types for security risks is dynamic and changes as Symantec discovers new categories. New categories are downloaded to the console or the client computer when new definitions arrive.

For Mac client computers, you can specify whether or not Symantec Endpoint Protection repairs the infected files that it finds. You can also specify whether Symantec Endpoint Protection moves the infected files that it cannot repair into the Quarantine. You can configure the settings for all administrator-defined scans or for Auto-Protect scans.

See "Managing the Quarantine" on page 363.

How Symantec Endpoint Protection acts on detections on Windows 8 computers

Symantec Endpoint Protection protects both the Windows 8 style user interface as well as the Windows 8 desktop. However, actions for the detections that are related to Windows 8 style apps and files function differently than actions for other detections.

The applications that are hosted on the Windows 8 style user interface are implemented in containers that are isolated from other processes in the operating system. Symantec Endpoint Protection does not clean or quarantine any detections that affect Windows 8 style apps or files. For any detections that involve these apps and files, Symantec Endpoint Protection only deletes or logs the detections.

For any detections that are not related to Windows 8 style apps and files, Symantec Endpoint Protection can quarantine and repair the detections and functions as it typically does on any other Windows operating system.

You should keep in mind the difference when setting up actions in Virus and Spyware Protection policy and when you run reports.

See "About the pop-up notifications that appear on the clients that run Windows 8" on page 370.

See "How Symantec Endpoint Protection handles detections of viruses and security risks" on page 339.

Setting up scheduled scans that run on Windows computers

You configure scheduled scans as part of a Virus and Spyware Protection policy. The scan settings are different for Windows clients and for Mac clients.

You can save your scheduled scan settings as a template. The scan templates can save you time when you configure multiple policies. You can use any scan that you save as a template as the basis for a new scan in a different policy. A scheduled scan template is included by default in the policy. The default scheduled scan scans all files and folders.

See "Managing scans on client computers" on page 323.

See "Customizing administrator-defined scans for the clients that run on Windows computers" on page 382.

See "Excluding file extensions from virus and spyware scans" on page 536.

Consider the following important points when you set up a scheduled scan:

Multiple simultaneous scans run serially	If you schedule multiple scans to occur on the same computer and the scans start at the same time, the scans run serially. After one scan finishes, another scan starts. For example, you might schedule three separate scans on your computer to occur at 1:00 P.M. Each scan scans a different drive. One scan scans drive C. Another scan scans drive D. Another scan scans drive E. In this example, a better solution is to create one scheduled scan that scans drives C, D, and E.
Missed scheduled scans might not run	If your computer misses a scheduled scan for some reason, by default Symantec Endpoint Protection tries to perform the scan until it starts or until a specific time interval expires. If Symantec Endpoint Protection cannot start the missed scan within the retry interval, it does not run the scan.
Scheduled scan time might drift	Symantec Endpoint Protection might not use the scheduled time if the last run of the scan occurred at a different time because of the scan duration or missed scheduled scan settings. For example, you might configure a weekly scan to run every Sunday at midnight and a retry interval of one day. If the computer misses the scan and starts up on Monday at 6am, the scan runs at 6am. The next scan is performed one week from Monday at 6am rather than the next Sunday at midnight.
	If you did not restart your computer until Tuesday at 6am, which is two days late and exceeds the retry interval, Symantec Endpoint Protection does not retry the scan. It waits until the next Sunday at midnight to try to run the scan.
	In either case, if you randomize the scan start time you might change the last run time of the scan.

You can click Help for more information about the options that are used in this procedure.

To set up scheduled scans that run on Windows computers

1   In the console, open a Virus and Spyware Protection policy.

2   Under **Windows Settings**, click **Administrator-defined Scans**.

3   On the **Scans** tab, under **Scheduled Scans**, click **Add**.

4   In the **Add Scheduled Scan** dialog box, click **Create a new scheduled scan**.

5   Click **OK**.

6   In the **Add Scheduled Scan** dialog box, on the **Scan Details** tab, type a name and description for this scheduled scan.

7   Click **Active Scan**, **Full Scan**, or **Custom Scan**.

8   If you selected **Custom**, under **Scanning**, you can specify the folders to scan.

9   Under **File types**, click **Scan all files** or **Scan only selected extensions**.

> **Note:** Scheduled scans always scan container files unless you disable the **Scan files inside compressed files** option under **Advanced Scanning Options** or you create specific exceptions for the container file extensions.

10 Under **Enhance the scan by checking**, check or uncheck **Memory**, **Common infection locations**, or **Well-known virus and security risk locations**.

11 On the **Schedule** tab, under **Scanning schedule**, set the frequency and the time at which the scan should run.

    The retry setting under **Missed Scheduled Scans** changes automatically according to whether you select **Daily**, **Weekly**, or **Monthly**.

12 Under **Missed Scheduled Scans**, you can disable the option to run a missed scan or you can change the retry interval.

    You can also specify a maximum scan duration before the scan pauses. You can also randomize scan start time.

13 If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.

14 Click **OK**.

Setting up scheduled scans that run on Mac computers

You configure scheduled scans as part of a Virus and Spyware Protection policy. The scan settings are different for Windows clients and for Mac clients.

See "Managing scans on client computers" on page 323.

See "Customizing administrator-defined scans for clients that run on Mac computers" on page 383.

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 Virus and Spyware Protection policy. The scan templates can save you time when you configure new policies or scans. A scheduled scan template is included by default in the policy. The default scheduled scan scans all files and directories.

To configure a scheduled scan for Mac clients

1   In the console, open a Virus and Spyware Protection policy.

2   Under **Mac Settings**, click **Administrator-defined Scans**.

3   On the **Scans** tab, under **Scheduled Scans**, click **Add**.

4   In the **Add Scheduled Scan** dialog box, click **Create a new scheduled scan**, and then click **OK**.

5   In the **Add Scheduled Scan** dialog box, on the **Scan Details** tab, type a name and a description for the scan.

6   Under **Scan drives and folders**, specify the items to scan.

7   Customize any settings, including scan priority.

8   On the **Schedule** tab, under **Scanning schedule**, set the frequency and the time at which the scan should run.

9   If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.

10 Click **OK**.

Running on-demand scans on client computers

You can run a manual, or on-demand, scan on client computers remotely from the management console. You might want to run an on-demand scan as part of your strategy to prevent and handle virus and spyware attacks on your client computers.

By default, an active scan runs automatically after you update definitions. You can configure an on-demand scan as a full scan or custom scan and then run the on-demand scan for more extensive scanning.

Settings for on-demand scans are similar to the settings for scheduled scans.

See "Managing scans on client computers" on page 323.

See "Preventing and handling virus and spyware attacks on client computers" on page 318.

For Windows client computers, you can run an active, full, or custom on-demand scan.

For Mac client computers, you can run only a custom on-demand scan.

The custom scan uses the settings that are configured for on-demand scans in the Virus and Spyware Protection policy.

Note: If you issue a restart command on a client computer that runs an on-demand scan, the scan stops, and the client computer restarts. The scan does not restart.

You can run an on-demand scan from the Computer Status log or from the **Clients** tab in the console.

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.

See "Running commands from the computer status log" on page 630.

See "About commands that you can run on client computers" on page 231.

To run an on-demand scan on client computers

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

2   Under **Clients**, right-click the clients or the group that you want to scan.

3   Do one of the following actions:

       ■   Click **Run Command on Group > Scan**.

       ■   Click **Run Command on Clients > Scan**.

4   For Windows clients, select **Active Scan**, **Full Scan**, or **Custom Scan**, and then click **OK**.

Adjusting scans to improve computer performance

By default, virus and spyware scans to minimize the effect on your client computers' resources. You can change some scan settings to optimize the performance even more. Many of the tasks that are suggested here are useful in the environments that run Symantec Endpoint Protection in guest operating systems on virtual machines (VMs).

The settings that are available are different for Windows computers and Mac computers.

See "Managing scans on client computers" on page 323.

Table 16-12 Adjusting scans to improve performance on Windows computers

Task	Description
Modify tuning and compressed files options for scheduled and on-demand scans	You can adjust the following options for scheduled and on-demand scans: ■ Change tuning options You can change the scan tuning to **Best Application Performance**. When you configure a scan with this setting, scans can start but they only run when the client computer is idle. If you configure an Active Scan to run when new definitions arrive, the scan might not run for up to 15 minutes if the user is using the computer. ■ Change the number of levels to scan compressed files The default level is 3. You might want to change the level to 1 or 2 to reduce scan time. See "Customizing administrator-defined scans for the clients that run on Windows computers" on page 382.
Use resumable scans	For computers in your network that have large volumes, scheduled scans can be configured as resumable scans. A scan duration option provides a specified period to run a scan. If the scan does not complete by the end of the specified duration, it resumes when the next scheduled scan period occurs. The scan resumes at the place where it stopped until the entire volume is scanned. Typically you use the scan duration option on servers. **Note:** Do not use a resumable scan if you suspect that the computer is infected. You should perform a full scan that runs until it scans the entire computer. You should also not use a resumable scan if a scan can complete before the specified interval. See "Setting up scheduled scans that run on Windows computers" on page 341.

Table 16-12   Adjusting scans to improve performance on Windows computers
(continued)

Task	Description
Adjust Auto-Protect settings	You can adjust some settings for Auto-Protect scans of the file system that might improve your client computers' performance. You can set the following options: ■ **File cache** Make sure the file cache is enabled (the default is enabled). When the file cache is enabled, Auto-Protect remembers clean files that it scanned and does not rescan them. ■ **Network settings** When Auto-Protect scans on remote computers is enabled, make sure that **Only when files are executed** is enabled. See "Customizing Auto-Protect for Windows clients" on page 378.
Allow all scans to skip trusted files	Virus and spyware scans include an option called Insight that skips trusted files. By default Insight is enabled. You can change the level of trust for the types of files that scans skip: ■ **Symantec and Community Trusted** This level skips files that are trusted by Symantec and the Symantec Community. ■ **Symantec Trusted** This level skips only files that are trusted by Symantec. See "Modifying global scan settings for Windows clients" on page 385.
Randomize scheduled scans	In virtualized environments, where multiple virtual machines (VMs) are deployed, simultaneous scans create resource problems. For example, a single server might run 100 or more VMs. Simultaneous scans on those VMs drain resources on the server. You can randomize scans to limit the impact on your server. See "Randomizing scans to improve computer performance in virtualized environments" on page 384.
Use Shared Insight Cache in virtualized environments	Shared Insight Cache eliminates the need to rescan the files that Symantec Endpoint Protection has determined are clean. You can used Shared Insight Cache for scheduled and manual scans on your clients computers. Shared Insight Cache is a separate application that you install on a server or in a virtual environment. See "Enabling or disabling the use of a network-based Shared Insight Cache" on page 656.

Table 16-12   Adjusting scans to improve performance on Windows computers
(continued)

Task	Description
Disable early launch anti-malware (ELAM) detection	Symantec Endpoint Protection ELAM works with Windows ELAM to provide protection against malicious startup drivers. See "Managing early launch anti-malware (ELAM) detections" on page 371.

Table 16-13   Adjusting scans to improve performance on Mac computers

Task	Description
Adjust scan priority	Applies to scheduled scans on clients that run on Mac computers. Scan priority on Mac computers is equivalent to tuning or performance adjustment on Windows computers. High priority means that the scan runs as fast as possible, but other applications may run more slowly during the scan. Low priority means that other applications run as fast as possible, but the scan may run more slowly. Medium priority balances the speed at which applications and scans run. See "Customizing administrator-defined scans for clients that run on Mac computers" on page 383.
Modify compressed files setting	Applies to Auto-Protect and on-demand scans. You can enable or disable the option, but you cannot specify the level of compressed files to scan. See "Customizing Auto-Protect for Mac clients" on page 379.

Adjusting scans to increase protection on your client computers

Symantec Endpoint Protection provides a high level of security by default. You can increase the protection even more. The settings are different for clients that run on Windows computers and clients that run on Mac computers.

Note: If you increase the protection on your client computers, you might impact computer performance.

Table 16-14 Adjusting scans to increase protection on Windows computers

Task	Description
Lock scan settings	Some settings are locked by default; you can lock additional settings so that users cannot change the protection on their computers.
Modify settings for administrator-defined scans	You should check or modify the following options: ■ Scan performance Set the scan tuning to **Best Scan Performance**. The setting, however, might affect your client computer performance. Scans run even if the computer is not idle. ■ Scheduled scan duration By default, scheduled scans run until the specified time interval expires and then resume when the client computer is idle. You can set the scan duration to **Scan until finished**. ■ Use Insight Lookup Insight Lookup uses the latest definition set from the cloud and information from the Insight reputation database to scan and make decisions about files. You should make sure that Insight Lookup is enabled. Insight Lookup settings are similar to the settings for Download Insight. See "Customizing administrator-defined scans for the clients that run on Windows computers" on page 382.
Specify stronger scan detection actions	Specify **Quarantine**, **Delete**, or **Terminate** actions for detections. **Note:** Be careful when you use **Delete** or **Terminate** for security risk detections. The action might cause some legitimate applications to lose functionality. See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 389.

Table 16-14   Adjusting scans to increase protection on Windows computers *(continued)*

Task	Description
Increase the level of Bloodhound protection	Bloodhound locates and isolates the logical regions of a file to detect virus-like behavior. You can change the detection level from **Automatic** to **Aggressive** to increase the protection on your computers. The **Aggressive** setting, however, is likely to produce more false positives. See "Modifying global scan settings for Windows clients" on page 385.
Adjust Auto-Protect settings	You can change the following options: ■ **File cache** You can disable the file cache so that Auto-Protect rescans good files. ■ **Network settings** By default, files on network drives are scanned only when they are executed. You can disable this option. See "Customizing Auto-Protect for Windows clients" on page 378.

Table 16-15   Adjusting scans to increase protection on Mac computers

Task	Description
Lock scan settings	Some settings are locked by default; you can lock additional settings so that users cannot change the protection on their computers.
Specify stronger scan detection actions	Specify **Quarantine**, **Delete**, or **Terminate** actions for detections. **Note:** Be careful when you use **Delete** or **Terminate** for security risk detections. The action might cause some legitimate applications to lose functionality. See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 389.

Managing Download Insight detections

Auto-Protect includes a feature that is called Download Insight, which examines the files that users try to download through Web browsers, text messaging clients, and other portals.

Supported portals include Internet Explorer, Firefox, Microsoft Outlook, Outlook Express, Google Chrome, Windows Live Messenger, and Yahoo Messenger.

Download Insight determines that a downloaded file might be a risk based on evidence about the file's reputation. Download Insight is supported only for the clients that run on Windows computers.

Note: If you install Auto-Protect for email on your client computers, Auto-Protect also scans the files that users receive as email attachments.

See "Managing scans on client computers" on page 323.

Table 16-16   Managing Download Insight detections

Task	Description
Learn how Download Insight uses reputation data to make decisions about files	Download Insight uses reputation information exclusively when it makes decisions about downloaded files. It does not use signatures or heuristics to make decisions. If Download Insight allows a file, Auto-Protect or SONAR scans the file when the user opens or runs the file. See "How Symantec Endpoint Protection uses reputation data to make decisions about files" on page 355.

Table 16-16   Managing Download Insight detections *(continued)*

Task	Description
View the Download Risk Distribution report to view Download Insight detections	You can use the Download Risk Distribution report to view the files that Download Insight detected on your client computers. You can sort the report by URL, Web domain, or application. You can also see whether a user chose to allow a detected file.
	Note: Risk details for a Download Insight detection show only the first portal application that attempted the download. For example, a user might use Internet Explorer to try to download a file that Download Insight detects. If the user then uses Firefox to try to download the file, the risk details show Internet Explorer as the portal.
	The user-allowed files that appear in the report might indicate false positive detections.
	You can also specify that you receive email notifications about new user-allowed downloads.
	See "Setting up administrator notifications" on page 642.
	Users can allow files by responding to notifications that appear for detections.
	Administrators receive the report as part of a weekly report that Symantec Endpoint Protection Manager generates and emails. You must have specified an email address for the administrator during installation or configured as part of the administrator properties. You can also generate the report from the **Reports** tab in the console.
	See "Running and customizing quick reports" on page 618.

Table 16-16   Managing Download Insight detections *(continued)*

Task	Description
Create exceptions for specific files or Web domains	You can create an exception for an application that your users download. You can also create an exception for a specific Web domain that you believe is trustworthy. See "Specifying how Symantec Endpoint Protection handles monitored applications" on page 537. See "Excluding a trusted Web domain from scans" on page 538. **Note:** If your client computers use a proxy with authentication, you must specify trusted Web domain exceptions for Symantec URLs. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites. For information about the recommended exceptions, see the following related knowledge base articles: ■ How to test connectivity to Insight and Symantec licensing servers ■ Required exclusions for proxy servers to allow Symantec Endpoint Protection to connect to Symantec reputation and licensing servers By default, Download Insight does not examine any files that users download from a trusted Internet or intranet site. You configure trusted sites and trusted local intranet sites on the **Windows Control Panel > Internet Options > Security** tab. When the **Automatically trust any file downloaded from an intranet site** option is enabled, Symantec Endpoint Protection allows any file that a user downloads from any sites in the lists. Symantec Endpoint Protection checks for updates to the Internet Options trusted sites list at user logon and every four hours. **Note:** Download Insight recognizes only explicitly configured trusted sites. Wildcards are allowed, but non-routable IP address ranges are not supported. For example, Download Insight does not recognize 10.*.*.* as a trusted site. Download Insight also does not support the sites that are discovered by the **Internet Options > Security > Automatically detect intranet network** option.
Make sure that Insight lookups are enabled	Download Insight requires reputation data from Symantec Insight to make decisions about files. If you disable Insight lookups, Download Insight runs but detects only the files with the worst reputations. Insight lookups are enabled by default. See "Enabling or disabling client submissions to Symantec Security Response" on page 359.

Table 16-16   Managing Download Insight detections *(continued)*

Task	Description
Customize Download Insight settings	You might want to customize Download Insight settings for the following reasons:
	■ Increase or decrease the number of Download Insight detections.
	You can adjust the malicious file sensitivity slider to increase or decrease the number of detections. At lower sensitivity levels, Download Insight detects fewer files as malicious and more files as unproven. Fewer detections are false positive detections.
	At higher sensitivity levels, Download Insight detects more files as malicious and fewer files as unproven. More detections are false positive detections.
	■ Change the action for malicious or unproven file detections.
	You can change how Download Insight handles malicious or unproven files. The specified action affects not only the detection but whether or not users can interact with the detection.
	For example, you might change the action for unproven files to **Ignore**. Then Download Insight always allows unproven files and does not alert the user.
	■ Alert users about Download Insight detections.
	When notifications are enabled, the malicious file sensitivity setting affects the number of notifications that users receive. If you increase the sensitivity, you increase the number of user notifications because the total number of detections increases.
	You can turn off notifications so that users do not have a choice when Download Insight makes a detection. If you keep notifications enabled, you can set the action for unproven files to **Ignore** so that these detections are always allowed and users are not notified.
	Regardless of the notifications setting, when Download Insight detects an unproven file and the action is **Prompt**, the user can allow or block the file. If the user allows the file, the file runs automatically.
	When notifications are enabled and Download Insight quarantines a file, the user can undo the quarantine action and allow the file.
	Note: If users allow a quarantined file, the file does not automatically run. The user can run the file from the temporary Internet folder. Typically the folder location is *drive:*\\Documents and Settings*username*\\Local Settings\\Temporary Internet Files.
	See "Customizing Download Insight settings" on page 388.
Allow clients to submit information about reputation detections to Symantec	By default, clients send information about reputation detections to Symantec.
	Symantec recommends that you enable submissions for reputation detections. The information helps Symantec address threats.
	See "Enabling or disabling client submissions to Symantec Security Response" on page 359.

How Symantec Endpoint Protection uses reputation data to make decisions about files

Symantec collects information about files from its global community of millions of users and its Global Intelligence Network. The collected information forms a reputation database that Symantec hosts. Symantec products leverage the information to protect client computers from new, targeted, and mutating threats. The data is sometimes referred to as being in the cloud since it does not reside on the client computer. The client computer must request or query the reputation database.

Symantec uses a technology it calls Insight to determine each file's level of risk or security rating.

Insight determines a file's security rating by examining the following characteristics of the file and its context:

- The source of the file
- How new the file is
- How common the file is in the community
- Other security metrics, such as how the file might be associated with malware

Scanning features in Symantec Endpoint Protection leverage Insight to make decisions about files and applications. Virus and Spyware Protection includes a feature that is called Download Insight. Download Insight relies on reputation information to make detections. If you disable Insight lookups, Download Insight runs but cannot make detections. Other protection features, such as Insight Lookup and SONAR, use reputation information to make detections; however, those features can use other technologies to make detections.

By default, a client computer sends information about reputation detections to Symantec Security Response for analysis. The information helps to refine Insight's reputation database. The more clients that submit information the more useful the reputation database becomes.

You can disable the submission of reputation information. Symantec recommends, however, that you keep submissions enabled.

Client computers also submit other types of information about detections to Symantec Security Response.

See "Managing Download Insight detections" on page 351.

See "How Symantec Endpoint Protection policy features work together" on page 356.

See "Enabling or disabling client submissions to Symantec Security Response" on page 359.

How Symantec Endpoint Protection policy features work together

Some policy features require each other to provide complete protection on Windows client computers.

Warning: Symantec recommends that you do not disable Insight lookups.

Table 16-17   How policy features work together

Feature	Interoperability Notes
Download Protection	Download Protection is part of Auto-Protect and gives Symantec Endpoint Protection the ability to track URLs. The URL tracking is required for several policy features. If you install Symantec Endpoint Protection without Download Protection, Download Insight has limited capability. Browser Intrusion Prevention and SONAR require Download Protection. The **Automatically trust any file downloaded from an intranet website** option also requires Download Protection.
Download Insight	Download Insight has the following dependencies: ■ Auto-Protect must be enabled If you disable Auto-Protect, Download Insight cannot function even if Download Insight is enabled. ■ Insight lookups must be enabled Symantec recommends that you keep the Insight lookups option enabled. If you disable the option, you disable Download Insight completely. **Note:** If basic Download Protection is not installed, Download Insight runs on the client at level 1. Any level that you set in the policy is not applied. The user also cannot adjust the sensitivity level. Even if you disable Download Insight, the **Automatically trust any file downloaded from an intranet website** option continues to function for Insight Lookup.

Table 16-17	How policy features work together *(continued)*
Feature	**Interoperability Notes**
Insight Lookup	Uses Insight lookups
	Insight Lookup uses the latest definitions from the cloud and the Insight reputation database to make decisions about files. If you disable Insight lookups, Insight Lookup uses the latest definitions only to make decisions about files.
	Insight Lookup also uses the **Automatically trust any file downloaded from an intranet website** option.
	Insight Lookup does not run on right-click scans of folders or drives on your client computers. However, Insight Lookup runs on right-click scans of selected files.
	Note: Insight Lookup uses the configured Insight Lookup slider level value to evaluate the files that were downloaded from a supported portal. If the files were not downloaded from a supported portal, then Insight Lookup detects them only if they have the worst reputation (similar to level 1).
SONAR	SONAR has the following dependencies:
	■ Download Protection must be installed.
	■ Auto-Protect must be enabled. If Auto-Protect is disabled, SONAR loses some detection functionality and appears to malfunction on the client. SONAR can detect heuristic threats, however, even if Auto-Protect is disabled.
	■ Insight lookups must be enabled. Without Insight lookups, SONAR can run but cannot make detections. In some rare cases, SONAR can make detections without Insight lookups. If Symantec Endpoint Protection has previously cached reputation information about particular files, SONAR might use the cached information.
Browser Intrusion Prevention	Download Protection must be installed. Download Insight can be enabled or disabled.
Trusted Web Domain exception	The exception is only applied if Download Protection is installed.

See "Managing Download Insight detections" on page 351.

See "Managing SONAR" on page 397.

See "Managing intrusion prevention on your client computers" on page 461.

About submitting information about detections to Symantec Security Response

You can configure your client computers to automatically submit information about detections to Symantec Security Response for analysis.

Symantec Response and the Global Intelligence Network use this submitted information to quickly formulate responses to new and developing security threats. The data that you submit improves Symantec's ability to respond to threats and customize protection. Symantec recommends that you always allow submissions.

See "About the types of threat protection that Symantec Endpoint Protection provides" on page 46.

You can choose to submit any of the following types of data:

■ File reputation
Information about the files that are detected based on their reputation. The information about these files contributes to the Symantec Insight reputation database to help protect your computers from new and emerging risks.

■ Antivirus detections
Information about virus and spyware scan detections.

■ Antivirus advanced heuristic detections
Information about potential threats that are detected by Bloodhound and other virus and spyware scan heuristics.
These detections are silent detections that do not appear in the Risk log. Information about these detections is used for statistical analysis.

■ SONAR detections
Information about threats that SONAR detects, which include high or low risk detections, system change events, and suspicious behavior from trusted applications.

■ SONAR heuristics
SONAR heuristic detections are silent detections that do not appear in the Risk log. This information is used for statistical analysis.

On the client, you can also manually submit a sample to Response from the Quarantine or through the Symantec Web site. To submit a file through the Symantec Web site, contact Symantec Technical Support.

See "Enabling or disabling client submissions to Symantec Security Response" on page 359.

See "How Symantec Endpoint Protection uses reputation data to make decisions about files" on page 355.

About submissions throttling

Symantec Endpoint Protection throttles client computer submissions to minimize any effect on your network. Symantec Endpoint Protection throttles submissions in the following ways:

- Client computers only send samples when the computer is idle. Idle submission helps randomize the submissions traffic across the network.

- Client computers send samples for unique files only. If Symantec has already seen the file, the client computer does not send the information.

- Symantec Endpoint Protection uses a Submission Control Data (SCD) file. Symantec publishes the SCD file and includes it as part of a LiveUpdate package. Each Symantec product has its own SCD file.

The SCD file controls the following settings:

- How many submissions a client can submit in one day

- How long to wait before the client software retries submissions

- How many times to retry failed submissions

- Which IP address of the Symantec Security Response server receives the submission

If the SCD file becomes out-of-date, then clients stop sending submissions. Symantec considers the SCD file out-of-date when a client computer has not retrieved LiveUpdate content in 7 days. The client stops sending submissions after 14 days.

If clients stop the transmission of the submissions, the client software does not collect the submission information and send it later. When clients start to transmit submissions again, they only send the information about the events that occur after the transmission restart.

Enabling or disabling client submissions to Symantec Security Response

Symantec Endpoint Protection can protect computers by submitting information about detections to Symantec Security Response. Symantec Security Response uses this information to address new and changing threats. Any data you submit

improves Symantec's ability to respond to threats and customize protection for your computers. Symantec recommends that you choose to submit as much detection information as possible.

Client computers submit information anonymously about detections. You can specify the types of detections for which clients submit information. You can also enable or disable submissions from client computers. Symantec recommends that you always enable submissions. In some cases, however, you might want to prevent your clients from submitting such information. For example, your corporate policies might prevent your client computers from sending any network information to outside entities.

To enable or disable client submissions to Symantec Security Response

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

2   In the **Settings** pane, click **External Communications Settings**.

3   Click the **Submissions** tab.

4   If you want to enable your client computers to submit data for analysis, check **Let computers automatically forward selected anonymous security information to Symantec**.

5   To disable submissions for the client, uncheck **Let computers automatically forward selected anonymous security information to Symantec**.

    If you disable submissions for a client and lock the settings, the user is unable to configure the client to send submissions. If you enable, select your submissions types and lock the settings, the user is not able to change your chosen settings. If you do not lock your settings, the user can change the configuration as desired.

    Symantec recommends that you submit threat information to help Symantec provide custom threat protection. You may need however, to disable this feature in response to network bandwidth issues or a restriction on data leaving the client. You can check the Client Activity to view log submissions activity if you need to monitor your bandwidth usage.

    See "Viewing logs" on page 624.

6   Select the types of information to submit:

    ■   File reputation
        Information about files that are detected based on their reputation. The information about these files contributes to the Symantec Insight reputation database to help protect your computers from new and emerging risks.

Note: Unmanaged clients require a paid license to enable the submission of file reputation data.

See "Licensing an unmanaged client" on page 123.

- Antivirus detections
  Information about virus and spyware scan detections.

- Antivirus advanced heuristic detections
  Information about the potential threats that are detected by Bloodhound and other virus and spyware scan heuristics.
  These detections are the silent detections that do not appear in the Risk log. Information about these detections is used for statistical analysis.

- SONAR detections
  Information about the threats that SONAR detects, which include high or low risk detections, system change events, and suspicious behavior from trusted applications.

- SONAR heuristics
  SONAR heuristic detections are silent detections that do not appear in the Risk log. This information is used for statistical analysis.

7 Check **Allow Insight lookups for threat detection** to allow Symantec Endpoint Protection to use the Symantec Insight reputation database to make decisions about threats.

Insight lookups are enabled by default. You can disable this option if you do not want to allow Symantec Endpoint Protection to query the Symantec Insight reputation database.

Download Insight, Insight Lookup, and SONAR use Insight lookups for threat detection. Symantec recommends that you allow Insight lookups. Disabling lookups disables Download Insight and may impair the functionality of SONAR heuristics and Insight Lookup.

See "About submitting information about detections to Symantec Security Response" on page 358.

See "How Symantec Endpoint Protection uses reputation data to make decisions about files" on page 355.

See "Specifying a proxy server for client submissions and other external communications" on page 362.

Specifying a proxy server for client submissions and other external communications

You can configure Symantec Endpoint Protection Manager to use a proxy server for submissions and other external communications that your Windows clients use.

To configure a proxy server for client submissions and other external communications

1 In the console, on the **Clients** page, select the group and then click **Policies**.

2 Under **Settings** or **Location-specific Settings**, click **External Communications**.

3 On the **Proxy Server (Windows)** tab, under **HTTPS Proxy Configuration**, select **Use custom proxy settings**.

4 Enter the information about the proxy server that your clients use. See the online Help for more information about the options.

5 Click **OK**.

Note: If your client computers use a proxy with authentication, you might need to specify exceptions for Symantec URLs in your proxy server configuration. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites.

You need to include exceptions for Symantec URLs in your proxy server settings if you use the following proxy configuration options:

■ You use a proxy server with authentication.

■ You select **Use a proxy server specified by my client browser** option in the Symantec Endpoint Protection Manager **External Communication Dialog**.

■ You use auto-detection or auto-configuration in your browser's Internet Options.

You do not have to specify exceptions for Symantec URLs in your proxy server settings if you do not use auto-detection or auto-configuration. You should select **Use custom proxy settings** in the **External Communication** dialog and then specify the authentication settings.

For information about the recommended exceptions, see the following knowledge base articles:

■ How to test connectivity to Insight and Symantec licensing servers

■ Required exclusions for proxy servers to allow Symantec Endpoint Protection to connect to Symantec reputation and licensing servers

See "Enabling or disabling client submissions to Symantec Security Response" on page 359.

See "Creating exceptions for Symantec Endpoint Protection" on page 530.

Managing the Quarantine

When virus and spyware scans detect a threat or SONAR detects a threat, Symantec Endpoint Protection places the files in the client computer's local Quarantine.

See "Managing scans on client computers" on page 323.

Table 16-18   Managing the Quarantine

Task	Description
Monitor files in the Quarantine	You should periodically check the quarantined files to prevent accumulating large numbers of files. Check the quarantined files when a new virus outbreak appears on the network. Leave files with unknown infections in the Quarantine. When the client receives new definitions, it rescans the items in the Quarantine and might delete or repair the file.
Delete files in the Quarantine	You can delete a quarantined file if a backup exists or if you have a copy of the file from a trustworthy source. You can delete a quarantined file directly on the infected computer or by using the Risk log in the Symantec Endpoint Protection console. See "Using the Risk log to delete quarantined files on your client computers" on page 367.
Configure how Symantec Endpoint Protection rescans items in the Quarantine when new definitions arrive	By default, Symantec Endpoint Protection rescans items in the Quarantine when new definitions arrive. It automatically repairs and restores items silently. Typically you should keep the default setting, but you can change the rescan action based on your needs. See "Configuring how the Quarantine handles the rescanning of files after new definitions arrive" on page 366.

Table 16-18   Managing the Quarantine *(continued)*

Task	Description
Specify how clients submit information about quarantined items	Symantec Endpoint Protection lets users submit infected or suspicious files and related side effects to Symantec Security Response for further analysis. When users submit information, Symantec can refine its detection and repair. You can enable signature-based detections in Quarantine to be forwarded from the local Quarantine to a Central Quarantine Server. Reputation detections in the local Quarantine cannot be sent to a Central Quarantine Server. You can configure the client to forward items if you use a Central Quarantine Server in your security network. The Central Quarantine Server can send the information to Symantec Security Response. Information that clients submit helps Symantec determine if a detected threat is real. Files that are submitted to Symantec Security Response become the property of Symantec Corporation. In some cases, files may be shared with the antivirus community. If Symantec shares files, Symantec uses industry-standard encryption and may make data anonymous to help protect the integrity of the content and your privacy. See "Configuring clients to submit quarantined items to a Central Quarantine Server or Symantec Security Response" on page 366.
Manage the storage of quarantined files	By default, the Quarantine stores backup, repaired, and quarantined files in a default folder. It automatically deletes files after 30 days. You can manage the storage of quarantined items in the following ways: ■ Specify a local folder to store quarantined files. You can use the default folder or a folder that you choose. See "Specifying a local Quarantine folder" on page 364. ■ Specify when files are automatically deleted. The Quarantine automatically deletes files after a specified number of days. You can also configure the Quarantine to delete files when the folder where the files are stored reaches a specified size. You can configure the settings individually for repaired files, backup files, and quarantined files. See "Specify when quarantined files are automatically deleted" on page 365.

Specifying a local Quarantine folder

If you do not want to use the default quarantine folder to store quarantined files on client computers, you can specify a different local folder. You can use path expansion by using the percent sign when you type the path. For example, you can type %COMMON_APPDATA%. Relative paths are not allowed.

See "Managing the Quarantine" on page 363.

To specify a local Quarantine folder

1   On the **Virus and Spyware Protection Policy** page, click **Quarantine**.

2   On the **Miscellaneous** tab, under **Local Quarantine Options**, click **Specify the quarantine folder**.

3   In the text box, type the name of a local folder on the client computers. You can use path expansion by using the percent sign when typing in the path. For example, you can type %COMMON_APPDATA%, but relative paths are not allowed.

4   If you are finished with the configuration for this policy, click **OK**.

Specify when quarantined files are automatically deleted

Symantec Endpoint Protection automatically deletes the files in the Quarantine when they exceed a specified age. You can configure the Quarantine to also delete files when the folder where they are stored reaches a certain size.

You can use one of the settings, or you can use both together. If you set both types of limits, then all files older than the time you have set are purged first. If the size of the folder still exceeds the size limit that you set, then the oldest files are deleted one by one. The files are deleted until the folder size falls below the specified limit.

See "Managing the Quarantine" on page 363.

To configure automatic clean-up options

1   In the console, open a Virus and Spyware Protection policy and click **Quarantine**.

2   On the **Cleanup** tab, under **Repaired files**, check or uncheck **Enable automatic deleting of repaired files**.

3   In the **Delete after** box, type a value or click an arrow to select the time interval in days.

4   Check **Delete oldest files to limit folder size at**, and then type in the maximum folder size, in megabytes. The default setting is 50 MB.

5   Under **Backup Files**, check or uncheck **Enable automatic deleting of backup files**.

6   In the **Delete after** box, type or click an arrow to select the time interval in days.

7   Check **Delete oldest files to limit folder size at**, and then type the maximum folder size, in megabytes. The default is 50 MB.

8   Under **Quarantined Files**, check or uncheck **Enable automatic deleting of quarantined files that could not be repaired**.

9   In the **Delete after** box, type a value or click an arrow to select the time interval in days.

10 Check **Delete oldest files to limit folder size at**, and then type in the maximum folder size, in megabytes. The default is 50 MB.

11 If you are finished with the configuration for this policy, click **OK**.

Configuring clients to submit quarantined items to a Central Quarantine Server or Symantec Security Response

Clients can automatically submit quarantine items to a Central Quarantine Server.

You can also allow users on client computers to manually submit quarantine items directly to Symantec Security Response.

See "Managing the Quarantine" on page 363.

To configure clients to submit quarantined items to a Central Quarantine Server or Symantec Security Response

1   In the console, open a Virus and Spyware Protection policy and click **Quarantine**.

2   Under **Quarantined Items**, do one or both of the following actions:

   ■   Select **Allow client computers to automatically submit quarantined items to a Quarantine Server**.
       Type the name of the Quarantine Server.
       Type the port number to use, and then select the number of seconds to retry connecting.

   ■   Select **Allow client computers to manually submit quarantined items to Symantec Security Response**.

3   If you are finished configuring settings for this policy, click **OK**.

Configuring how the Quarantine handles the rescanning of files after new definitions arrive

You can configure the actions that you want to take when new definitions arrive on client computers. By default, the client rescans items in the Quarantine and automatically repairs and restores items silently. Typically, you should always use this setting.

If you created an exception for a file or application in the Quarantine, Symantec Endpoint Protection restores the file after new definitions arrive.

See "Managing the Quarantine" on page 363.

To configure how the Quarantine handles the rescanning of files after new definitions arrive

1   In the console, open a Virus and Spyware Protection policy and click **Quarantine**.

2   On the **General** tab, under **When New Virus Definitions Arrive**, click one of the following options:

    ■   **Automatically repair and restore files in Quarantine silently**

    ■   **Repair files in Quarantine silently without restoring**

    ■   **Prompt user**

    ■   **Do nothing**

3   If you are finished with the configuration for this policy, click **OK**.

Using the Risk log to delete quarantined files on your client computers

You can use the Risk log in the Symantec Endpoint Protection Manager console to delete quarantined files on your client computers. You run the **Delete from Quarantine** command from the log for any quarantined file that you want to delete.

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. To successfully delete all risks in a compressed file, you must select all the files in the compressed file.

To use the Risk log to delete files from the Quarantine on your client computers

1   Click **Monitors**.

2   On the **Logs** tab, from the **Log type** list box, select the **Risk** log, and then click **View Log**.

3   Do one of the following actions:

    ■   Select an entry in the log that has a file that has been quarantined.

    ■   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**.

Managing the virus and spyware notifications that appear on client computers

You can decide whether or not notifications appear on client computers for virus and spyware events. You can customize messages about detections.

See "Managing scans on client computers" on page 323.

Table 16-19 Tasks for managing virus and spyware notifications that appear on client computers

Task	Description
Customize a scan detection message	For Windows client computers, you can configure a detection message for the following types of scans: ■ All types of Auto-Protect, including Download Insight ■ Scheduled scans and on-demand scans For scheduled scans, you can configure a separate message for each scan. **Note:** If a process continually downloads the same security risk to a client computer, Auto-Protect automatically stops sending notifications after three detections. Auto-Protect also stops logging the event. In some situations, however, Auto-Protect does not stop sending notifications and logging events. Auto-Protect continues to send notifications and log events when the action for the detection is Leave alone (log only). For Mac client computers, you can configure a detection message that applies to all scheduled scans and a message that applies to on-demand scans. See "Customizing administrator-defined scans for the clients that run on Windows computers" on page 382. See "Customizing administrator-defined scans for clients that run on Mac computers" on page 383.
Change settings for user notifications about Download Insight detections	You can change what notifications users receive about Download Insight detections. See "Managing Download Insight detections" on page 351.
Change settings for user notifications about SONAR detections	You can change what notifications users receive about SONAR detections. See "Managing SONAR" on page 397.

Table 16-19   Tasks for managing virus and spyware notifications that appear on client computers *(continued)*

Task	Description
Choose whether or not to display the Auto-Protect results dialog	Applies to Windows client computers only.
	Applies to Auto-Protect for the file system only.
	See "Customizing administrator-defined scans for the clients that run on Windows computers" on page 382.
Set up Auto-Protect email notifications	Applies to Windows client computers only.
	when Auto-Protect email scans find a risk, Auto-Protect can send email notifications to alert the email sender and any other email address that you specify. You can also insert a warning into the email message.
	For Internet Email Auto-Protect, you can also specify that a notification appears about scan progress when Auto-Protect scans an email.
	See "Customizing Auto-Protect for email scans on Windows computers" on page 380.
Allow users to see scan progress and start or stop scans	Applies to Windows client computers only.
	You can configure whether or not the scan progress dialog box appears. You can configure whether or not users are allowed to pause or delay scans.
	When you let users view scan progress, a link to the scan progress dialog appears in the main pages of the client user interface. A link to reschedule the next scheduled scan also appears.
	See "Allowing users to view scan progress and interact with scans" on page 391.
Configure warnings, error, and prompts	Applies to Windows client computers only.
	You can enable or disable several types of alerts that appear on client computers about Virus and Spyware Protection events.
	See "Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers" on page 386.
Enable or disable popup notifications on the Windows 8 style user interface	Applies to clients that run on Windows 8.
	You can enable or disable the popup notifications that appear in the Windows 8 style user interface for detections and other critical events.
	See "Enabling or disabling Symantec Endpoint Protection pop-up notifications on Windows 8 clients" on page 370.

About the pop-up notifications that appear on the clients that run Windows 8

On Windows 8 computers, pop-up notifications for malware detections and other critical Symantec Endpoint Protection events appear on the Windows 8 style user interface and the Windows 8 desktop. The notifications alert the user to an event that occurred in either the Windows 8 style user interface or the Windows 8 desktop, regardless of which interface the user is currently viewing.

You can enable or disable the pop-up notifications on your client computers.

Note: The Windows 8 configuration also includes settings to show or hide notifications. Symantec Endpoint Protection pop-up notifications only appear if Windows 8 is configured to show them. In the Windows 8 style user interface, the **Settings** pane or the **Change PC Settings** option let you show or hide app notifications. See the Windows 8 user documentation for more information.

If the user clicks a notification on the Windows 8 style user interface, the Windows 8 desktop appears. If the user clicks the notification on the Windows 8 desktop, the notification disappears. For detections of malware or security risks, the user can view information about the detections in the **Detection Results** dialog on the Windows 8 desktop.

When Symantec Endpoint Protection notifies Windows 8 that it detected malware or a security risk that affects a Windows 8 style app, an alert icon appears on the app tile. When the user clicks the tile, the Windows App Store appears so that the user can re-download the app.

See "Enabling or disabling Symantec Endpoint Protection pop-up notifications on Windows 8 clients" on page 370.

See "How Symantec Endpoint Protection acts on detections on Windows 8 computers" on page 341.

Enabling or disabling Symantec Endpoint Protection pop-up notifications on Windows 8 clients

By default pop-up notifications appear on the Windows 8 style user interface and the Windows 8 desktop for malware detections and other critical Symantec Endpoint Protection events.

The user can view the Windows desktop to see details about the event that produced the notification. The user might need to take an action such as

re-download an app. In some cases, however, you might want to hide these pop-up notifications from users. You can enable or disable this type of notification in the Symantec Endpoint Protection configuration.

Note: The Windows 8 configuration also includes settings to show or hide notifications. Symantec Endpoint Protection notifications only appear if Windows 8 is configured to show them. On the Windows 8 style user interface, the **Settings** pane or the **Change PC Settings** option let you show or hide app notifications. See the Windows 8 user documentation for more information.

To enable or disable Symantec Endpoint Protection notifications on Windows 8 clients

1 In the console, on the **Clients** tab, on the **Policies** tab, under **Location-specific settings**, next to **Client User Interface Control Settings**, click **Server Control**.

2 Next to **Server Control**, click **Customize**.

3 In the **Client User Interface Settings** dialog, under **General**, check or uncheck **Enable Windows toast notifications**.

4 Click **OK**.

See "About the pop-up notifications that appear on the clients that run Windows 8" on page 370.

Managing early launch anti-malware (ELAM) detections

Early launch anti-malware (ELAM) provides protection for the computers in your network when they start up and before third-party drivers initialize. Malicious software can load as a driver or rootkits might attack before the operating system completely loads and Symantec Endpoint Protection starts. Rootkits can sometimes hide themselves from virus and spyware scans. Early launch anti-malware detects these rootkits and bad drivers at startup.

Symantec Endpoint Protection provides an ELAM driver that works with the Windows ELAM driver to provide the protection. The Windows ELAM driver must be enabled for the Symantec ELAM driver to have any affect.

You use the Windows Group Policy editor to view and modify the Windows ELAM settings. See your Windows 8 documentation for more information.

Table 16-20   Managing ELAM detections

Task	Description
View the status of ELAM on your client computers	You can see whether Symantec Endpoint Protection ELAM is enabled in the Computer Status log. See "Viewing logs" on page 624.
View ELAM detections	You can view early launch anti-malware detections in the Risk log. When Symantec Endpoint Protection ELAM is configured to report detections of bad or bad critical drivers as unknown to Windows, Symantec Endpoint Protection logs the detections as **Log only**. By default, Windows ELAM allows unknown drivers to load. See "Viewing logs" on page 624.
Enable or disable ELAM	You might want to disable Symantec Endpoint Protection ELAM to help improve computer performance. See "Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options" on page 373. See "Adjusting scans to improve computer performance" on page 346.
Adjust ELAM detection settings if you get false positives	The Symantec Endpoint Protection ELAM settings provide an option to treat bad drivers and bad critical drivers as unknown. Bad critical drivers are the drivers that are identified as malware but are required for computer startup. You might want to select the override option if you get false positive detections that block an important driver. If you block an important driver, you might prevent client computers from starting up. **Note:** ELAM does not support a specific exception for an individual driver. The override option applies globally to ELAM detections. See "Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options" on page 373.
Run the Power Eraser tool on ELAM detections that Symantec Endpoint Protection cannot remediate	In some cases, an ELAM detection requires the Symantec Power Eraser tool that is part of the Symantec Help tool. See "Troubleshooting computer issues with the Symantec Help support tool" on page 755.

Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options

Symantec Endpoint Protection provides an ELAM driver that works with the Microsoft ELAM driver to provide protection for the computers in your network when they start up. The settings are supported on Microsoft Windows 8.

The Symantec Endpoint Protection ELAM driver is a special type of driver that initializes first and inspects other startup drivers for malicious code. When the driver detects a startup driver, it determines whether the driver is good, bad, or unknown. The Symantec Endpoint Protection driver then passes the information to Windows to decide to allow or block the detected driver.

You cannot create exceptions for individual ELAM detections; however, you can create a global exception to log all bad drivers as unknown. By default, unknown drivers are allowed to load.

For some ELAM detections that require remediation, you might be required to run Power Eraser. Power Eraser is part of the Symantec Help tool.

Note: Auto-Protect scans any driver that loads.

To adjust the Symantec Endpoint Protection ELAM options

1   In the Symantec Endpoint Protection Manager console, on the **Policies** tab, open a Virus and Spyware Protection policy.

2   Under **Protection Technologies**, select **Early Launch Anti-Malware Driver**.

3   Check or uncheck **Enable Symantec early launch anti-malware**.

   The Windows ELAM driver must be enabled for this option to be enabled. You use the Windows Group Policy editor to view and modify the Windows ELAM settings. See your Windows 8 documentation for more information.

4   If you want to log the detections only, under **Detection Settings**, select **Log the detection as unknown so that Windows allows the driver to load**.

5   Click **OK**.

See "Managing early launch anti-malware (ELAM) detections" on page 371.

See "Troubleshooting computer issues with the Symantec Help support tool" on page 755.

Customizing scans

This chapter includes the following topics:

- Customizing the virus and spyware scans that run on Windows computers

- Customizing the virus and spyware scans that run on Mac computers

- Customizing Auto-Protect for Windows clients

- Customizing Auto-Protect for Mac clients

- Customizing Auto-Protect for email scans on Windows computers

- Customizing administrator-defined scans for the clients that run on Windows computers

- Customizing administrator-defined scans for clients that run on Mac computers

- Randomizing scans to improve computer performance in virtualized environments

- Modifying global scan settings for Windows clients

- Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers

- Customizing Download Insight settings

- Changing the action that Symantec Endpoint Protection takes when it makes a detection

- Allowing users to view scan progress and interact with scans

- How Symantec Endpoint Protection interacts with Windows Security Center

Customizing the virus and spyware scans that run on Windows computers

You can customize options for administrator-defined scans (scheduled and on-demand scans) that run on Windows computers. You can also customize options for Auto-Protect.

See "Managing scans on client computers" on page 323.

Table 17-1   Customizing virus and spyware scans on Windows computers

Task	Description
Customize Auto-Protect settings	You can customize Auto-Protect in many ways, including the configuration for the following settings: ■ The types of files that Auto-Protect scans ■ The actions that Auto-Protect takes when it makes a detection ■ The user notifications for Auto-Protect detections You can also enable or disable the **Scan Results** dialog for Auto-Protect scans of the file system. See "Customizing Auto-Protect for Windows clients" on page 378. See "Customizing Auto-Protect for email scans on Windows computers" on page 380.
Customize administrator-defined scans	You can customize the following types of options for scheduled and on-demand scans. ■ Compressed files ■ Tuning options ■ Insight Lookup ■ Advanced schedule options ■ User notifications about detections See "Customizing administrator-defined scans for the clients that run on Windows computers" on page 382. You can also customize scan actions.
Adjust ELAM settings	You might want to enable or disable Symantec Endpoint Protection early launch anti-malware (ELAM) detection if you think ELAM is affecting your computers' performance. Or you might want to override the default detection setting if you get many false positive ELAM detections. See "Managing early launch anti-malware (ELAM) detections" on page 371.

Table 17-1 Customizing virus and spyware scans on Windows computers
(continued)

Task	Description
Adjust Download Insight settings	You might want to adjust the malicious file sensitivity to increase or decrease the number of detections. You can also modify actions for detections and user notifications for detections. See "Customizing Download Insight settings" on page 388.
Customize scan actions	You can change the action that Symantec Endpoint Protection takes when it makes a detection. See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 389.
Customize global scan settings	You might want to customize global scan settings to increase or decrease the protection on your client computers. See "Modifying global scan settings for Windows clients" on page 385.
Customize miscellaneous options for Virus and Spyware Protection	You can specify the types of risk events that clients send to Symantec Endpoint Protection Manager. You can also adjust how Symantec Endpoint Protection interacts with Windows Security Center. See "Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers" on page 386. See "How Symantec Endpoint Protection interacts with Windows Security Center" on page 393.

Customizing the virus and spyware scans that run on Mac computers

You can customize options for administrator-defined scans (scheduled and on-demand scans) that run on Mac computers. You can also customize options for Auto-Protect.

See "Managing scans on client computers" on page 323.

Table 17-2 Customizing the virus and spyware scans that run on Mac computers

Task	Description
Customize Auto-Protect	You can customize Auto-Protect settings for the clients that run on Mac computers. See "Customizing Auto-Protect for Mac clients" on page 379.

Table 17-2 Customizing the virus and spyware scans that run on Mac computers *(continued)*

Task	Description
Customize administrator-defined scans	You can customize common settings and notifications as well as scan priority.
	You can also enable or disable a warning to alert the user when definitions are out-of-date.
	See "Customizing administrator-defined scans for clients that run on Mac computers" on page 383.

Customizing Auto-Protect for Windows clients

You might want to customize Auto-Protect settings for Windows clients.

See "Customizing the virus and spyware scans that run on Windows computers" on page 376.

See "Managing scans on client computers" on page 323.

To configure Auto-Protect for Windows clients

1 In the console, open a Virus and Spyware Protection policy.

2 Under **Windows Settings**, under **Protection Technology**, click **Auto-Protect**.

3 On the **Scan Details** tab, check or uncheck **Enable Auto-Protect**.

> **Note:** If you disable Auto-Protect, Download Insight cannot function even if it is enabled.

4 Under **Scanning**, under **File types**, click one of the following options:

 ■ **Scan all files**
   This option is the default and is the most secure option.

 ■ **Scan only selected extensions**
   You can improve scan performance by selecting this option, however, you might decrease the protection on your computer.

5 Under **Additional options**, check or uncheck **Scan for security risks**.

6 Click **Advanced Scanning and Monitoring** to change options for the actions that trigger Auto-Protect scans and how Auto-Protect handles scans of floppy disks.

7 Click **OK**.

8   Under **Network Settings**, check or uncheck **Scan files on remote computers** to enable or disable Auto-Protect scans of network files.

   By default, Auto-Protect scans files on remote computers only when the files are executed.

   You might want to disable network scanning to improve scan and computer performance.

9   When file scans on remote computers is enabled, click **Network Settings** to modify network scanning options.

10 In the **Network Settings** dialog box, do any of the following actions:

   ■ Enable or disable Auto-Protect to trust files on the remote computers that run Auto-Protect.

   ■ Configure network cache options for Auto-Protect scans.

11 Click **OK**.

12 On the **Actions** tab, set any of the options.

   See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 389.

   You can also set remediation options for Auto-Protect.

13 On the **Notifications** tab, set any of the notification options.

   See "Managing the virus and spyware notifications that appear on client computers" on page 368.

14 On the **Advanced** tab, set any of the following options:

   ■ **Startup and shutdown**

   ■ **Reload options**

15 Under **Additional Options**, click **File Cache** or **Risk Tracer**.

16 Configure the file cache or Risk Tracer settings, and then click **OK**.

17 If you are finished with the configuration for this policy, click **OK**.

Customizing Auto-Protect for Mac clients

You might want to customize Auto-Protect settings for the clients that run on Mac computers.

See "Customizing the virus and spyware scans that run on Mac computers" on page 377.

See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 389.

See "Managing the virus and spyware notifications that appear on client computers" on page 368.

To customize Auto-Protect for Mac clients

1   In the console, open a Virus and Spyware Protection policy.

2   Under **Mac Settings**, under **Protection Technology**, click **File System Auto-Protect**.

3   At the top of the **Scan Details** tab, click the lock icon to lock or unlock all settings.

4   Check or uncheck any of the following options:

    ■   **Enable File System Auto-Protect**

    ■   **Automatically repair infected files**

    ■   **Quarantine files that cannot be repaired**

    ■   **Scan compressed files**

5   Under **General Scan Details**, specify the files that Auto-Protect scans.

    Note: To exclude files from the scan, you must select **Scan everywhere except in specified folders**, and then add an Exceptions policy to specify the files to exclude.

    See "Excluding a file or a folder from scans" on page 534.

    ---

6   Under **Scan Mounted Disk Details**, check or uncheck any of the available options.

7   On the **Notifications** tab, set any of the notification options, and then click **OK**.

Customizing Auto-Protect for email scans on Windows computers

You can customize Auto-Protect for email scans on Windows computers.

See "Customizing the virus and spyware scans that run on Windows computers" on page 376.

See "Managing the virus and spyware notifications that appear on client computers" on page 368.

To customize Auto-Protect for email scans on Windows computers

1   In the console, open a Virus and Spyware Protection policy.

2   Under **Windows Settings**, click one of the following options:

    ■ **Internet Email Auto-Protect**

    ■ **Microsoft Outlook Auto-Protect**

    ■ **Lotus Notes Auto-Protect**

3   On the **Scan Details** tab, check or uncheck **Enable Internet Email Auto-Protect**.

4   Under **Scanning**, under **File types**, click one of the following options:

    ■ **Scan all files**
        This option is the default and most secure option.

    ■ **Scan only selected extensions**
        You can improve scan performance by selecting this option, however, you might decrease the protection on your computer.

5   Check or uncheck **Scan files inside compressed files**.

6   On the **Actions** tab, set any of the options.

    See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 389.

7   On the **Notifications** tab, under **Notifications**, check or uncheck **Display a notification message on the infected computer**. You can also customize the message.

8   Under **Email Notifications**, check or uncheck any of the following options:

    ■ **Insert a warning into the email message**

    ■ **Send email to the sender**

    ■ **Send email to others**

    You can customize the message text and include a warning. For Internet Email Auto-Protect you must also specify the mail server.

9   For Internet Email Auto-Protect only, on the **Advanced** tab, under **Encrypted Connections**, enable or disable encrypted POP3 or SMTP connections.

10 Under **Mass Mailing Worm Heuristics**, check or uncheck **Outbound worm heuristics**.

11 If you are finished with the configuration for this policy, click **OK**.

Customizing administrator-defined scans for the clients that run on Windows computers

You might want to customize scheduled or on-demand scans for the clients that run on Windows computers. You can set options for scans of compressed files and optimize the scan for computer or scan performance.

See "Customizing the virus and spyware scans that run on Windows computers" on page 376.

See "Setting up scheduled scans that run on Windows computers" on page 341.

To customize an administrator-defined scan for the clients that run on Windows computers

1 In the console, open a Virus and Spyware Protection policy.

2 Under **Windows Settings**, click **Administrator-defined scans**.

3 Do one of the following actions:

■ Under **Scheduled Scans**, select the scheduled scan that you want to customize, or create a new scheduled scan.

■ Under **Administrator On-demand Scan**, click **Edit**.

4 On the **Scan Details** tab, select **Advanced Scanning Options**.

5 On the **Compressed Files** tab, you can reduce the number of levels to scan compressed files. If you reduce the number of levels, you might improve client computer performance.

6 On the **Tuning** tab, change the tuning level for the best client computer performance or the best scan performance.

7 Click **OK**.

8 On the **Insight Lookup** tab, change any of the settings to adjust how Insight Lookup handles reputation detections. The settings are similar to the settings for Download Insight.

9 For scheduled scans only, on the **Schedule** tab, set any of the following options:

■ **Scan Duration**

You can set how long the scan runs before it pauses and waits until the client computer is idle. You can also randomize scan start time.

- **Missed Scheduled Scans**
  You can specify a retry interval for missed scans.

10 On the **Actions** tab, change any detection actions.

See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 389.

11 On the **Notifications** tab, enable or disable a notification that appears on client computers when the scan makes a detection.

See "Managing the virus and spyware notifications that appear on client computers" on page 368.

12 Click **OK**.

Customizing administrator-defined scans for clients that run on Mac computers

You customize scheduled scans and on-demand scans separately. Some of the options are different.

See "Customizing the virus and spyware scans that run on Mac computers" on page 377.

See "Setting up scheduled scans that run on Mac computers" on page 344.

See "Changing the action that Symantec Endpoint Protection takes when it makes a detection" on page 389.

See "Managing the virus and spyware notifications that appear on client computers" on page 368.

To customize a scheduled scan that runs on Mac computers

1 In the console, open a Virus and Spyware Protection policy.

2 Under **Mac Settings**, select **Administrator-Defined Scans**.

3 Under **Scheduled Scans**, select the scheduled scan that you want to customize, or create a new scheduled scan.

4 On the **Scan Details** tab, under **Scan drives and folders**, select the items that you want to scan.

5 Set the scan priority.

6   Click **OK**.

Edit the scan details for any other scan that is included in this policy.

7   On the **Notifications** tab, enable or disable notification messages about scan detections. The setting applies to all scheduled scans that you include in this policy.

8   On the **Common Settings** tab, set any of the following options:

   ■   **Scan Options**

   ■   **Actions**

   ■   **Alerts**

   These options apply to all scheduled scans that you include in this policy.

9   Click **OK**.

To customize the on-demand scans that run on Mac computers

1   On the Virus and Spyware Protection Policy page, under **Mac Settings**, select **Administrator-Defined Scans**.

2   Under **Administrator On-demand Scan**, click **Edit**.

3   On the **Scan Details** tab, under **Scan Drives and Folders**, select the items that you want to scan.

   You can also specify actions for scan detections and enable or disables scans of compressed files.

4   On the **Notifications** tab, enable or disable notifications for detections. You can also specify the message that appears.

5   Click **OK**.

Randomizing scans to improve computer performance in virtualized environments

You can randomize scheduled scans to improve performance on Windows client computers. Randomization is important in virtualized environments.

For example, you might schedule scans to run at 8:00 PM. If you select a four-hour time interval, scans on client computers start at a randomized time between 8:00 PM and 12:00 AM.

See "Adjusting scans to improve computer performance" on page 346.

See "Setting up scheduled scans that run on Windows computers" on page 341.

To randomize scans to improve computer performance in virtualized environments

1   In the console, open a Virus and Spyware Protection policy and click
    Administrator-defined Scans.

2   Create a new scheduled scan or select an existing scheduled scan to edit.

3   In the **Add Scheduled Scan** or **Edit Scheduled Scan** dialog box, click the
    Schedule tab.

4   Under **Scanning Schedule**, select how often the scan should run.

5   Under **Scan Duration**, check **Scan for up to** and select the number of hours.
    The number of hours controls the time interval during which scans are
    randomized.

6   Make sure that you enable **Randomize scan start time within this period
    (recommended in VMs)**

7   Click **OK**.

8   Make sure that you apply the policy to the group that includes the computers
    that run Virtual Machines.

Modifying global scan settings for Windows clients

You can customize global settings for the scans that run on Windows client
computers. You might want to modify these options to increase security on your
client computers.

Note: If you increase the protection on your client computers by modifying these
options, you might affect client computer performance.

See "Managing scans on client computers" on page 323.

See "Customizing the virus and spyware scans that run on Windows computers"
on page 376.

To modify global scan settings for Windows clients

1   In the console, open a Virus and Spyware Protection policy.

2   Under **Windows Settings**, click **Global Scan Options**.

3 Configure any of the following options:

Insight	Insight allows scans to skip trusted good files. The scan can skip the files that Symantec trusts as good (more secure) or that the community trusts as good (less secure).
Bloodhound	Bloodhound isolates and locates the logical regions of a file to detect a high percentage of unknown viruses. Bloodhound then analyzes the program logic for virus-like behavior. You can specify how the sensitivity for detection.
Password for mapped network drives	Specifies whether or not clients prompt users for a password when the client scans network drives.

4 Click **OK**.

Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers

Each Virus and Spyware Protection policy includes the options that apply to all virus and spyware scans that run on Windows client computers.

See "Customizing the virus and spyware scans that run on Windows computers" on page 376.

See "How Symantec Endpoint Protection interacts with Windows Security Center" on page 393.

See "Managing the virus and spyware notifications that appear on client computers" on page 368.

Windows Security Center	You can specify how Windows Security Center works with Symantec Endpoint Protection.
Internet Browser Protection	You can specify a default URL that Symantec Endpoint Protection uses when it repairs a security risk that changed a browser home page.

Risk log events	By default, clients always send certain types of events to the management server (such as **Scan stopped** or **Scan started**). You can choose to send or not send other types of events (such as **File not scanned**).
	The events that clients send to the management server affect information in reports and logs. You should decide what types of events that you want to forward to the management server. You can reduce the size of the logs and the amount of information that is included in reports if you select only certain types of events.
	You can also configure how long the client retains log items. The option does not affect any events that the clients send to the management console. You can use the option to reduce the actual log size on the client computers.
	You can also specify how often client computers send aggregated events to the management server.
Miscellaneous notifications	You can configure the following notifications:
	■ Warn users when definitions are out-of-date or missing You can display and customize warning messages to appear on client computers when their virus and security risk definitions are outdated or missing. You might want to alert users if you do not have automatic updates scheduled.
	■ Include a URL in the error messages that appear during scans In rare cases, users might see errors appear on their client computers during scans. For example, the client computer might encounter buffer overruns or decompression problems. You can specify a URL that points to the Symantec support Web site or to a custom URL. For example, you might have an internal Web site that you want to specify instead. **Note:** The URL also appears in the System event log for the client on which the error occurs.

Virtual image exceptions	You can exclude virtual images from Auto-Protect or administrator-defined scans. You must create the baseline images that you want to exclude with the Virtual Image Exclusion tool.

To modify miscellaneous settings for Virus and Spyware Protection

1   In the console, open a Virus and Spyware Protection policy.

2   Under **Windows Settings**, click **Miscellaneous**.

Specify options for Windows Security Center or Internet Browser Protection.

3   On the **Log Handling** tab, set options for event filtering, log retention, and log aggregation.

4   On the **Notifications** tab, configure global notifications.

5   On the **Virtual Images** tab, configure virtual image exceptions.

6   Click **OK**.

Customizing Download Insight settings

You might want to customize Download Insight settings to decrease false positive detections on client computers. You can change how sensitive Download Insight is to the file reputation data that it uses to characterize malicious files. You can also change the notifications that Download Insight displays on client computers when it makes a detection.

See "Customizing the virus and spyware scans that run on Windows computers" on page 376.

See "Managing Download Insight detections" on page 351.

To customize Download Insight settings

1   In the console, open a Virus and Spyware Protection policy and select **Download Protection**.

2   On the **Download Insight** tab, make sure that **Enable Download Insight to detect potential risks in downloaded files based on file reputation** is checked.

If Auto-Protect is disabled, Download Insight cannot function even if it is enabled.

3   Move the slider for malicious file sensitivity to the appropriate level.

If you set the level higher, Download Insight detects more files as malicious and fewer files as unproven. Higher settings, however, return more false positives.

4   Check or uncheck the following options to use as additional criteria for examining unproven files:

- **Files with fewer than x users**

- **Files known by users for less than x days**

When unproven files meet this criteria, Download Insight detects the files as malicious.

5   Make sure that **Automatically trust any file downloaded from an intranet website** is checked.

6   On the **Actions** tab, under **Malicious Files**, specify a first action and a second action.

7   Under **Unproven Files**, specify the action.

8   On the **Notifications** tab, you can specify whether or not to display a message on client computers when Download Insight makes a detection.

You can also customize the text of a warning message that appears when a user allows a file that Download Insight detects.

9   Click **OK**.

Changing the action that Symantec Endpoint Protection takes when it makes a detection

You can configure the action or actions that scans should take when they make a detection. Each scan has its own set of actions, such as Clean, Quarantine, Delete, or Leave alone (log only).

On Windows clients, each detection category can be configured with a first action and a second action in case the first action is not possible.

See "Customizing the virus and spyware scans that run on Windows computers" on page 376.

See "Customizing the virus and spyware scans that run on Mac computers" on page 377.

See "Managing Download Insight detections" on page 351.

See "Managing SONAR" on page 397.

See "Checking the scan action and rescanning the identified computers" on page 322.

See "Remediating risks on the computers in your network" on page 320.

By default, Symantec Endpoint Protection tries to clean a file that a virus infected. If Symantec Endpoint Protection cannot clean a file, it performs the following actions:

■ Moves the file to the Quarantine on the infected computer and denies any access to the file.

■ Logs the event.

By default, Symantec Endpoint Protection moves any files that security risks infect into the Quarantine.

If you set the action to log only, by default if users create or save infected files, Symantec Endpoint Protection deletes them.

On Windows computers, you can also configure remediation actions for administrator scans, on-demand scans, and Auto-Protect scans of the file system.

You can lock actions so that users cannot change the action on the client computers that use this policy.

Warning: For security risks, use the Delete action with caution. In some cases, deleting security risks causes applications to lose functionality. If you configure the client to delete the files that security risks affect, it cannot restore the files.

To back up the files that security risks affect, use the Quarantine action instead.

To change the action that Symantec Endpoint Protection takes when it makes a detection on Windows computers

1   In the console, open a Virus and Spyware Protection policy, and then select the scan (any Auto-Protect scan, administrator scan, or on-demand scan).

2   On the **Actions** tab, under **Detection**, select a type of malware or security risk.

By default, each subcategory is automatically configured to use the actions that are set for the entire category.

Note: The categories change dynamically over time as Symantec gets new information about risks.

---

3   To configure actions for a subcategory only, do one of the following actions:

■ Check **Override actions configured for Malware**, and then set the actions for that subcategory only.

> **Note:** There might be a single subcategory under a category, depending on how Symantec currently classifies risks. For example, under **Malware**, there might be a single subcategory called Viruses.

- Check **Override actions configured for Security Risks**, and then set the actions for that subcategory only.

4 Under **Actions for**, select the first and second actions that the client software takes when it detects that category of virus or security risk.

For security risks, use the Delete action with caution. In some cases, deleting security risks causes applications to lose functionality.

5 Repeat these steps for each category for which you want to set actions (viruses and security risks).

6 When you finish configuring this policy, click **OK**.

To specify the action that Symantec Endpoint Protection takes when it makes a detection on Mac computers

1 In the Virus and Spyware Protection policy, under **Mac Settings**, select **Administrator-Defined Scans**.

2 Do one of the following actions:

- For scheduled scans, select the **Common Settings** tab.

- For on-demand scans, on the **Scans** tab, under **Administrator On-demand Scan**, click **Edit**.

3 Under **Actions**, check either of the following options:

- **Automatically repair infected files**

- **Quarantine files that cannot be repaired**

4 For on-demand scans, click **OK**.

5 When you finish configuring this policy, click **OK**.

Allowing users to view scan progress and interact with scans

You can configure whether or not the scan progress dialog box appears on client computers. If you allow the dialog box to appear on client computers, users are always allowed to pause or delay an administrator-defined scan.

When you allow users to view scan progress, a link appears in the main pages of the client UI to display scan progress for the currently running scan. A link to reschedule the next scheduled scan also appears.

When you allow users to view scan progress, the following options appear in the main pages of the client UI:

■ When a scan runs, the message link *scan* **in progress** appears.
The user can click the link to display the scan progress.

■ A link to reschedule the next scheduled scan also appears.

See "Managing scans on client computers" on page 323.

You can allow users to stop a scan entirely. You can also configure options for how users pause or delay scans.

You can allow the user to perform the following scan actions:

Pause	When a user pauses a scan, the Scan Results dialog box remains open and waits for the user to either continue or abort the scan. If the computer is turned off, the paused scan does not continue.
Snooze	When a user snoozes a scheduled scan, the user has the option of snoozing the scan for one hour or three hours. The number of snoozes is configurable. When a scan snoozes, the Scan Results dialog box closes; it reappears when the snooze period ends and the scan resumes.
Stop	When a user stops a scan, the scan usually stops immediately. If a user stops a scan while the client software scans a compressed file, the scan does not stop immediately. In this case, the scan stops as soon as the compressed file has been scanned. A stopped scan does not restart.

A paused scan automatically restarts after a specified time interval elapses.

You can click Help for more information about the options that are used in this procedure.

To allow users to view scan progress and interact with scans

1 In the console, open a Virus and Spyware Protection policy and click **Administrator-defined Scans**.

2 On the **Advanced** tab, under **Scan Progress Options**, click **Show scan progress** or **Show scan progress if risk detected**.

3 To automatically close the scan progress indicator after the scan completes, check **Close the scan progress window when done**.

4 Check **Allow user to stop scan**.

5 Click **Pause Options**.

6 In the **Scan Pause Options** dialog box, do any of the following actions:

- To limit the time that a user may pause a scan, check **Limit the time the scan may be paused**, and then type a number of minutes. The range is 3 to 180.

- To limit the number of times a user may delay (or snooze) a scan, in the **Maximum number of snooze opportunities** box, type a number between 1 and 8.

- By default, a user can delay a scan for one hour. To change this limit to three hours, check **Allow users to snooze the scan for 3 hours**.

7 Click **OK**.

How Symantec Endpoint Protection interacts with Windows Security Center

Windows Security Center provides alerts on your client computers if any security software is out of date or if security settings should be strengthened. It is included with Windows XP Service Pack 2 or higher and Windows Vista. You can use a Virus and Spyware Protection policy to configure Windows Security Center settings on your client computers that run Windows XP Service Pack 2 or Service Pack 3. The settings do not apply to clients that run Windows Vista.

See "Customizing administrator-defined scans for the clients that run on Windows computers" on page 382.

Note: The settings do not apply to Windows Action Center in Windows 7 and Windows 8.

Table 17-3   Options to configure how Windows Security Center works with the client

Option	Description	When to use
Disable Windows Security Center	Lets you permanently or temporarily disable Windows Security Center on your client computers Available options: ■ Never. Windows Security Center is always enabled on the client computer. ■ Once. Windows Security Center is disabled only once. If a user enables it, it is not disabled again. ■ Always. Windows Security Center is permanently disabled on the client computer. If a user enables it, it is immediately disabled. ■ Restore. Windows Security Center is enabled if the Virus and Spyware Protection Policy previously disabled it.	Disable Windows Security Center permanently if you do not want your client users to receive the security alerts that it provides. Client users can still receive Symantec Endpoint Protection alerts. Enable Windows Security Center permanently if you want your client users to receive the security alerts that it provides. You can set Windows Security Center to display Symantec Endpoint Protection alerts.
Display antivirus alerts within Windows Security Center	Lets you set antivirus alerts from the Symantec Endpoint Protection client to appear in the Windows notification area.	Enable this setting if you want your users to receive Symantec Endpoint Protection alerts with other security alerts in the Windows notification area of their computers.
Display a Windows Security Center message when definitions are outdated	Lets you set the number of days after which Windows Security Center considers definitions to be outdated. By default, Windows Security Center sends this message after 30 days.	Set this option if you want Windows Security Center to notify your client users about outdated definitions more frequently than the default time (30 days). **Note:** On client computers, Symantec Endpoint Protection checks every 15 minutes to compare the out-of-date time, the date of the definitions, and the current date. Typically, no out-of-date status is reported to Windows Security Center because definitions are usually updated automatically. If you update definitions manually you might have to wait up to 15 minutes to view an accurate status in Windows Security Center.

Managing SONAR

This chapter includes the following topics:

- About SONAR

- Managing SONAR

- Handling and preventing SONAR false positive detections

- Adjusting SONAR settings on your client computers

- Monitoring SONAR detection results to check for false positives

- Managing TruScan proactive threat scans for legacy clients

About SONAR

SONAR is a real-time protection that detects potentially malicious applications when they run on your computers. SONAR provides "zero-day" protection because it detects threats before traditional virus and spyware detection definitions have been created to address the threats.

SONAR uses heuristics as well as reputation data to detect emerging and unknown threats. SONAR provides an additional level of protection on your client computers and complements your existing Virus and Spyware Protection, intrusion prevention, and firewall protection.

SONAR uses a heuristics system that leverages Symantec's online intelligence network with proactive local monitoring on your client computers to detect emerging threats. SONAR also detects changes or behavior on your client computers that you should monitor.

Note: Auto-Protect also uses a type of heuristic that is called Bloodhound to detect suspicious behavior in files.

SONAR might inject some code into the applications that run in Windows user mode to monitor them for suspicious activity. In some cases, the injection might affect the application performance or cause problems with running the application. You can create an exception to exclude the file, folder, or application from this type of monitoring.

Note: SONAR does not inject code into applications on Symantec Endpoint Protection 12.1 or earlier clients. If you use Symantec Endpoint Protection Manager 12.1.2 to manage clients, a SONAR file exception in an Exceptions policy is ignored on your legacy clients. If you use a legacy Symantec Endpoint Protection Manager to manage clients, the legacy policy does not support SONAR file exceptions for your Symantec Endpoint Protection 12.1.2 clients. You can prevent SONAR code injection into applications on these clients, however, by creating an **Application to monitor** exception in the legacy policy. After the client learns the application, you can configure an application exception in the policy.

Symantec Endpoint Protection clients version 12.0 or earlier do not support SONAR; however, legacy clients use TruScan proactive threat scans to provide protection against zero-day threats. TruScan proactive threat scans run periodically rather than in real time.

SONAR does not make detections on application type, but on how a process behaves. SONAR acts on an application only if that application behaves maliciously, regardless of its type. For example, if a Trojan horse or keylogger does not act maliciously, SONAR does not detect it.

SONAR detects the following items:

Heuristic threats	SONAR uses heuristics to determine if an unknown file behaves suspiciously and might be a high risk or low risk. It also uses reputation data to determine whether the threat is a high risk or low risk.
System changes	SONAR detects applications or the files that try to modify DNS settings or a host file on a client computer.
Trusted applications that exhibit bad behavior	Some good trusted files might be associated with suspicious behavior. SONAR detects these files as suspicious behavior events. For example, a well-known document sharing application might create executable files.

If you disable Auto-Protect, you limit SONAR's ability to make detections of high and low risk files. If you disable Insight lookups (reputation queries), you also limit the SONAR's detection capability.

Managing SONAR

SONAR is part of Proactive Threat Protection on your client computers. You manage SONAR settings as part of a Virus and Spyware Protection policy.

You configure SONAR settings for the clients that run Symantec Endpoint Protection version 12.1. SONAR settings also include TruScan proactive threat scan settings for legacy clients. Many of the settings can be locked so that users on client computers cannot change the settings.

Table 18-1   Managing SONAR

Task	Description
Learn how SONAR works	Learn how SONAR detects unknown threats. Information about how SONAR works can help you make decisions about using SONAR in your security network. See "About SONAR" on page 395.
Check that SONAR is enabled	To provide the most complete protection for your client computers you should enable SONAR. SONAR interoperates with some other Symantec Endpoint Protection features. SONAR requires Auto-Protect. You can use the Clients tab to check whether Proactive Threat Protection is enabled on your client computers. **Note:** Legacy clients do not report Proactive Threat Protection status to Symantec Endpoint Protection Manager. See "Adjusting SONAR settings on your client computers" on page 402.
Check the default settings for SONAR	SONAR settings are part of a Virus and Spyware Protection policy. See "About the default Virus and Spyware Protection policy scan settings" on page 336.

Table 18-1 Managing SONAR *(continued)*

Task	Description
Make sure that Insight lookups are enabled	SONAR uses reputation data in addition to heuristics to make detections. If you disable Insight lookups, SONAR makes detections by using heuristics only. The rate of false positives might increase, and the protection that SONAR provides is limited.
	You enable or disable Insight Lookups in the **Submissions** dialog.
	See "Enabling or disabling client submissions to Symantec Security Response" on page 359.
Monitor SONAR events to check for false positive detections	You can use the SONAR log to monitor events.
	You can also view the SONAR Detection Results report (under Risk Reports) to view information about detections.
	See "Monitoring SONAR detection results to check for false positives" on page 404.
	See "Monitoring endpoint protection" on page 603.
Adjust SONAR settings	You can change the detection action for some types of threats that SONAR detects. You might want to change the detection action to reduce false positive detections.
	You also might want to enable or disable notifications for high or low risk heuristic detections.
	See "Adjusting SONAR settings on your client computers" on page 402.
	See "Handling and preventing SONAR false positive detections" on page 400.

Table 18-1   Managing SONAR *(continued)*

Task	Description
Prevent SONAR from detecting the applications that you know are safe	SONAR might detect the files or applications that you want to run on your client computers. You can use an Exceptions policy to specify exceptions for the specific files, folders, or applications that you want to allow. For the items that SONAR quarantines, you can create an exception for the quarantined item from the SONAR log.
	You also might want to set SONAR actions to log and allow detections. You can use application learning so that Symantec Endpoint Protection learns the legitimate applications on your client computers. After Symantec Endpoint Protection learns the applications that you use in your network, you can change the SONAR action to Quarantine.
	Note: If you set the action for high risk detections to log only, you might allow potential threats on your client computers.
	See "Handling and preventing SONAR false positive detections" on page 400.
Prevent SONAR from examining some applications	In some cases an application might become unstable or cannot run when SONAR injects code into the application to examine it. You can create a file, folder, or application exception for the application.
	See "Creating exceptions for Symantec Endpoint Protection" on page 530.
Manage the way SONAR detects the applications that make DNS or host file changes	You can use the SONAR policy settings to globally adjust the way SONAR handles detections of DNS or host file changes. You can use the Exceptions policy to configure exceptions for specific applications.
	See "Adjusting SONAR settings on your client computers" on page 402.
	See "Creating an exception for an application that makes a DNS or host file change" on page 540.

Table 18-1   Managing SONAR *(continued)*

Task	Description
Manage TruScan proactive threat scans for legacy clients	Symantec Endpoint Protection clients version 12.0 or earlier do not support SONAR; these clients use TruScan proactive threat scans.. You can adjust TruScan proactive threat scan settings to change the scan actions, sensitivity, and frequency. You might want to adjust the settings to handle false positive detections on your legacy client computers. See "About adjusting TruScan settings for legacy clients" on page 406. See "Configuring TruScan proactive threat scan settings for legacy clients" on page 408.
Allow clients to submit information about SONAR detections to Symantec	Symantec recommends that you enable submissions on your client computers. The information that clients submit about detections helps Symantec address threats. The information helps Symantec create better heuristics, which results in fewer false positive detections. See "Enabling or disabling client submissions to Symantec Security Response" on page 359.

Handling and preventing SONAR false positive detections

SONAR might make false positive detections for certain internal custom applications. Also, if you disable Insight lookups, the number of false positives from SONAR increases.

See "Enabling or disabling client submissions to Symantec Security Response" on page 359.

You can change SONAR settings to mitigate false positive detections in general. You can also create exceptions for a specific file or a specific application that SONAR detects as a false positive.

You can also adjust settings and create exceptions for TruScan proactive threat scans, which run on Symantec Endpoint Protection clients version 12.0 or earlier. See "Managing TruScan proactive threat scans for legacy clients" on page 405.

Warning: If you set the action for high risk detections to log only, you might allow potential threats on your client computers.

Table 18-2   Handling SONAR false positives

Task	Description
Log SONAR high risk heuristic detections and use application learning	You might want to set detection action for high risk heuristic detections to **Log** for a short period of time. Let application learning run for the same period of time. Symantec Endpoint Protection learns the legitimate processes that you run in your network. Some true detections might not be quarantined, however.
	See "Configuring the management server to collect information about the applications that the client computers run" on page 313.
	After the period of time, you should set the detection action back to **Quarantine**.
	Note: If you use aggressive mode for low risk heuristic detections, you increase the likelihood of false positive detections. Aggressive mode is disabled by default.
	See "Adjusting SONAR settings on your client computers" on page 402.

Table 18-2   Handling SONAR false positives *(continued)*

Task	Description
Create exceptions for SONAR to allow safe applications	You can create exceptions for SONAR in the following ways:
	■ Use the SONAR log to create an exception for an application that was detected and quarantined
	You can create an exception from the SONAR log for false positive detections. If the item is quarantined, Symantec Endpoint Protection restores the item after it rescans the item in the Quarantine. Items in the Quarantine are rescanned after the client receives updated definitions.
	See "Creating exceptions from log events in Symantec Endpoint Protection Manager" on page 541.
	See "Configuring how the Quarantine handles the rescanning of files after new definitions arrive" on page 366.
	■ Use an Exceptions policy to specify an exception for a particular file name, folder name, or application.
	You can exclude an entire folder from SONAR detection. You might want to exclude the folders where your custom applications reside.
	See "Creating exceptions for Symantec Endpoint Protection" on page 530.

Adjusting SONAR settings on your client computers

You might want to change the SONAR actions to reduce the rate of false positive detections. You might also want to change the SONAR actions to change the number of detection notifications that appear on your client computers.

Note: The settings for SONAR notifications are also used for TruScan proactive threat scan notifications.

To adjust SONAR settings on your client computers

1   In the Virus and Spyware Protection policy, select **SONAR**.

2   Make sure that **Enable SONAR** is checked.

3   Under **Scan Details**, change the actions for high or low risk heuristic threats.

     You can enable aggressive mode for low risk detections. This setting increases SONAR sensitivity to low risk detections. It might increase the false positive detections.

4   Optionally change the settings for the notifications that appear on your client computers.

     The SONAR settings also control notifications for TruScan proactive threat scans.

5   Under **System Change Events**, change the action for either **DNS change detected** or **Host file change detected**.

> **Note:** The **Prompt** action might result in many notifications on your client computers. Any action other than **Ignore** might result in many log events in the console and email notifications to administrators.

> **Warning:** If you set the action to **Block**, you might block important applications on your client computers.

     For example, if you set the action to **Block** for **DNS change detected**, you might block VPN clients. If you set the action to **Block** for **Host file change detected**, you might block your applications that need to access the host file. You can use a DNS or host file change exception to allow a specific application to make DNS or host file changes.

     See "Creating an exception for an application that makes a DNS or host file change" on page 540.

6   Under **Suspicious Behavior Detection**, change the action for high or low risk detections.

7   Click **OK**.

See "Managing SONAR" on page 397.

See "Creating exceptions for Symantec Endpoint Protection" on page 530.

Monitoring SONAR detection results to check for false positives

The client collects and uploads SONAR detection results to the management server. The results are saved in the SONAR log.

To determine which processes are legitimate and which are security risks, look at the following columns in the log:

Event	The event type and the action that the client has taken on the process, such as cleaning it or logging it. Look for the following event types: ■ A possible legitimate process is listed as a **Potential risk found** event. ■ A probable security risk is listed as a **Security risk found** event.
Application	The process name.
Application type	The type of malware that SONAR or a TruScan proactive threat scan detected.
File/Path	The path name from where the process was launched.

The **Event** column tells you immediately whether a detected process is a security risk or a possible legitimate process. However, a potential risk that is found may or may not be a legitimate process, and a security risk that is found may or may not be a malicious process. Therefore, you need to look at the **Application type** and **File/Path** columns for more information. For example, you might recognize the application name of a legitimate application that a third-party company has developed.

Legacy clients do not support SONAR. Legacy clients collect similar events from TruScan proactive threat scans, however, and include them in the SONAR log.

To monitor SONAR detection results to check for false positives

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

2 On the Logs tab, in the **Log type** drop-down list, click **SONAR**.

3 Select a time from the **Time range** list box closest to when you last changed a scan setting.

4 Click **Advanced Settings**.

5 In the **Event type** drop-down list, select one of the following log events:

■ To view all detected processes, make sure **All** is selected.

■ To view the processes that have been evaluated as security risks, click **Security risk found**.

■ To view the processes that have been evaluated and logged as potential risks, click **Potential risk found**.

6 Click **View Log**.

7 After you identify the legitimate applications and the security risks, create an exception for them in an Exceptions policy.

You can create the exception directly from the SONAR Logs pane.

See "Creating exceptions from log events in Symantec Endpoint Protection Manager" on page 541.

Managing TruScan proactive threat scans for legacy clients

You can manage TruScan proactive threat scans by using two different implementation approaches. Each approach offers the advantages that relate to your network size, security features, and the workload that your technical support staff shares.

With either approach, you typically need to create exceptions for false positive detections.

Table 18-3   Managing TruScan proactive threat scans on legacy clients

Task	Description
Use the Symantec default settings	The Symantec default settings provide a high level of protection and require a low level of management. When you first install the Symantec Endpoint Protection Manager, use the default settings.
	Using the Symantec defaults, the client software determines the action and the sensitivity level. The scan engine that runs on the client computer automatically quarantines the security risks and logs potential risks and unknown risks.
	Use the Symantec default settings for the first two to four weeks after you set up the management server.

Table 18-3   Managing TruScan proactive threat scans on legacy clients
                      (continued)

Task	Description
Adjust the default settings manually.	After the initial break-in period during which you become more familiar with the technology, you may want more control. If you use this approach, you adjust the detection action and sensitivity level yourself.
	When you disable the Symantec defaults, you specify a single response action for detections, whether or not they are risks. For example, a scan can quarantine all the detected processes or log all the detected processes, but a scan does not do both.

See "About adjusting TruScan settings for legacy clients" on page 406.

See "Configuring TruScan proactive threat scan settings for legacy clients" on page 408.

See "Creating exceptions for Symantec Endpoint Protection" on page 530.

About adjusting TruScan settings for legacy clients

Typically, you should use Symantec defaults for TruScan proactive threat scans. However, when you first set up your network, you might want to adjust the settings manually.

Table 18-4   Adjusting TruScan settings for legacy clients

Setting	Description
Action	As a best practice, when you first start to manage the scans yourself, set the action to **Log**. This means that neither the security risks nor the legitimate processes use the action that you ultimately want. You want the scans to quarantine or terminate security risks and to ignore the legitimate processes.
	Create exceptions for any false positive detection. The exceptions define the process and the action to take when a scan detects a specified process.

Table 18-4   Adjusting TruScan settings for legacy clients *(continued)*

Setting	Description
Sensitivity	When you first adjust the sensitivity level for Trojan horses and worms, set the sensitivity level to 10. When the sensitivity level is low, the scans detect fewer processes than with the sensitivity level set higher. The rate of legitimate processes that are logged as potential risks is low. After you run the sensitivity level at 10 for a few days and monitor the log for any legitimate applications, you can raise the sensitivity level to 20. Over a 60-day to 90-day period, you can gradually increase the sensitivity level in 10-unit increments to 100. For maximum protection, leave the sensitivity level at 100.
	By using this gradual break-in approach, the users on the client computers are not overwhelmed with detection notifications as soon as you deploy the client. Instead, you can allocate time to monitor the increase in notifications at each level.
	For keyloggers, start the sensitivity level on Low.
	As you increase the sensitivity level, more processes are detected, both malicious and legitimate. The sensitivity level does not appreciably affect the rate of logged legitimate processes. A higher sensitivity level means that a scan flags a higher quantity of processes that are security risks as well as legitimate processes. But the ratio of legitimate to malicious processes remains nearly constant, despite the sensitivity level. Furthermore, the sensitivity level does not indicate the level of certainty that is associated with a detection. For example, a scan may detect one process at sensitivity level 10 and detect another process at sensitivity level 90. But the sensitivity level does not mean that one process is more of a threat than the other.
	After you change the sensitivity level of the scans, use the SONAR log to determine whether the sensitivity level is too low or too high. If the client reports many legitimate processes as security risks, then you may want to set the sensitivity level lower. You can increase the level after you create exceptions for the legitimate processes.
	Note: After you have added all the exceptions to an Exceptions policy, it is likely that any new detections are security risks. For greater security, you can change the response action for all processes back to either **Quarantine** or **Terminate**. Continue to monitor the SONAR log in case the scan detects and quarantines new legitimate applications.
Scan frequency	The default frequency for scans is one hour. If the performance of the client computers becomes too slow, decrease the scan frequency.

Configuring TruScan proactive threat scan settings for legacy clients

Legacy clients cannot use SONAR settings. Instead, legacy clients use TruScan to detect unknown threats.

By default, TruScan proactive threat scans detect Trojan horses, worms, and keyloggers. Also by default the detection response and sensitivity is determined by Symantec. For example, a detected process can be quarantined or logged. If you choose to configure the actions manually, you set a single action for detections. A detected process would always be quarantined or always logged depending on the action that you choose.

You can also set the action for commercial application detections.

Typically, you should not modify the default settings.

Note: You control user notifications for TruScan detections on the SONAR **Scan Details** tab.

To configure TruScan proactive threat scan settings for legacy clients

1   In the Virus and Spyware Protection policy, click **SONAR**.

2   Select **TruScan Legacy Client Settings**.

    By default, the **Scan Details**, **Detecting Commercial Applications**, and **Frequency** settings are hidden.

3   Click the arrow icon to expand the settings for **Scan Details**.

4   Check or uncheck **Scan for trojans and worms** and **Scan for keyloggers**.

5   To change the actions or sensitivity for either risk type, uncheck **Use defaults defined by Symantec**.

    Notifications are sent automatically if an action is set to **Quarantine** or **Terminate**. Use the **Terminate** action with caution. In some cases, you can cause an application to lose functionality.

6   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**.

7   Click the arrow icon to expand the settings for **Detecting Commercial Applications**.

8   Set the action for commercial keyloggers or commercial remote control programs.

9 Click the arrow to expand the settings for **Scan Frequency**.

10 Set one of the following options:

- At the default scanning frequency
  The scan engine software determines the scan frequency. This option is the default setting.

- At a custom scanning frequency
  If you enable this option, you can specify that the client scans new processes immediately when it detects them. You can also configure the scan frequency time.

11 Click **OK**.

See "Managing TruScan proactive threat scans for legacy clients" on page 405.

See "About adjusting TruScan settings for legacy clients" on page 406.

Managing Tamper Protection

This chapter includes the following topics:

■ About Tamper Protection

■ Changing Tamper Protection settings

About Tamper Protection

Tamper Protection provides real-time protection for Symantec applications that run on servers and clients. It prevents non-Symantec processes such as worms, Trojan horses, viruses, and security risks, from affecting Symantec resources. You can configure the software to block or log attempts to modify Symantec resources.

Note: Tamper Protection runs on Windows clients only. It does not run on Mac clients.

By default, Tamper Protection is enabled and is set to **Block and do not log**. You can change the setting to **Log only** or **Block and log** if you want to monitor the detections for false positives. Tamper Protection can generate many log messages, so you might not want to log the events.

If you use any third-party security risk scanners that detect and defend against unwanted adware and spyware, these scanners typically affect Symantec resources. If you set Tamper Protection to log tamper events when you run such a scanner, Tamper Protection generates a large number of log entries. If you decide to log Tamper Protection events, use log filtering to manage the number of events.

You can create exceptions for the applications that Tamper Protection detects.

Changing Tamper Protection settings

Tamper Protection provides real-time protection for Symantec applications that run on servers and clients. It prevents threats and security risks from tampering with Symantec resources. You can enable or disable Tamper Protection. You can also configure the action that Tamper Protection takes when it detects a tampering attempt on the Symantec resources in your network.

Tamper Protection settings are configured globally for a selected group.

To change Tamper Protection settings

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

2   On the **Policies** tab, under **Settings**, click **General Settings**.

3   On the **Tamper Protection** tab, check or uncheck **Protect Symantec security software from being tampered with or shut down**.

4   In the list box under **Actions to take if an application attempts to tamper with or shut down Symantec security software**, select one of the following actions:

   ■   **Log only**

   ■   **Block and do not log**

   ■   **Block and log**

5   Click the icon to lock or unlock the options on client computers. When you lock an option, you prevent user changes to the option.

6   Click **OK**.

See "About Tamper Protection" on page 411.

Managing firewall protection

This chapter includes the following topics:

- Managing firewall protection
- Creating a firewall policy
- Managing firewall rules
- Setting up firewall rules

Managing firewall protection

The firewall allows the incoming network traffic and outgoing network traffic that you specify in firewall policy. The Symantec Endpoint Protection firewall policy contains rules and protection settings, most of which you can enable or disable and configure.

Table 20-1 describes ways in which you can manage your firewall protection. All of these tasks are optional.

Table 20-1   Manage firewall protection

Task	Description
Read about firewall protection	Before you configure your firewall protection, you should familiarize yourself with the firewall. See "How a firewall works" on page 415. See "About the Symantec Endpoint Protection firewall" on page 415.

Table 20-1   Manage firewall protection *(continued)*

Task	Description
Create a firewall policy	Symantec Endpoint Protection installs with a default firewall policy. You can modify the default policy or create new ones.
	You must create a policy first before you configure firewall rules and firewall protection settings for that policy.
	See "Creating a firewall policy" on page 416.
	See "Enabling and disabling a firewall policy" on page 420.
Create and customize firewall rules	Firewall rules are the policy components that control how the firewall protects client computers from malicious attacks.
	The default firewall policy contains default firewall rules. And when you create a new policy, Symantec Endpoint Protection provides default firewall rules. However, you can modify the default rules or create new ones.
	See "Managing firewall rules" on page 428.
	See "Setting up firewall rules" on page 446.
Enable firewall protection settings	After the firewall has completed certain operations, control is passed to a number of components. Each component is designed to perform a different type of packet analysis.
	See "Automatically allowing communications for essential network services" on page 420.
	See "Automatically blocking connections to an attacking computer" on page 422.
	See "Detecting potential attacks and spoofing attempts" on page 423.
	See "Preventing stealth detection" on page 424.
	See "Disabling the Windows firewall" on page 425.
	See "Configuring peer-to-peer authentication" on page 426.
Monitor firewall protection	Regularly monitor the firewall protection status on your computers.
	See "Monitoring endpoint protection" on page 603.

See "Running commands on the client computer from the console" on page 233.

See "Configuring firewall settings for mixed control" on page 421.

See the knowledge base article Symantec Endpoint Protection Network Threat Protection (Firewall) Overview and Best Practices White Paper.

How a firewall works

A firewall does all of the following tasks:

- Prevents any unauthorized users from accessing the computers and networks in your organization that connect to the Internet

- Monitors the communication between your computers and other computers on the Internet

- Creates a shield that allows or blocks attempts to access the information on your computer

- Warns you of connection attempts from other computers

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

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

Packets contain information about the following:

- Sending computers

- Intended recipients

- How the packet data is processed

- Ports that receive the packets

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

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

See "About the Symantec Endpoint Protection firewall" on page 415.

See "Managing firewall protection" on page 413.

About the Symantec Endpoint Protection firewall

The Symantec Endpoint Protection firewall uses firewall policies and rules to allow or block network traffic. The Symantec Endpoint Protection includes a default Firewall policy with default firewall rules and firewall settings for the office environment. The office environment is normally under the protection of

corporate firewalls, boundary packet filters, or antivirus servers. Therefore, it is normally more secure than most home environments, where limited boundary protection is available.

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. The firewall also uses stateful inspection of all network traffic.

When you install the console for the first time, it adds a default Firewall policy to each group automatically.

Every time you add a new location, the console copies a Firewall policy to the default location automatically.

You determine the level of interaction that you want users to have with the client by permitting or blocking their ability to configure firewall rules and firewall settings. Users can interact with the client only when it notifies them of new network connections and possible problems. Or they can have full access to the user interface.

You can enable or disable the firewall protection as needed.

You can install the client with default firewall settings. In most cases you do not have to change the settings. However, if you have a detailed understanding of networks, you can make many changes in the client firewall to fine-tune the client computer's protection.

See "Managing firewall protection" on page 413.

See "How a firewall works" on page 415.

See "How the firewall uses stateful inspection" on page 434.

See "The types of security policies" on page 293.

Creating a firewall policy

The Symantec Endpoint Protection includes a default Firewall policy with default firewall rules and default firewall settings for the office environment. The office environment is normally under the protection of corporate firewalls, boundary packet filters, or antivirus servers. Therefore, it is normally more secure than most home environments, where limited boundary protection is available.

When you install the console for the first time, it adds a default Firewall policy to each group automatically.

Every time you add a new location, the console copies a Firewall policy to the default location automatically. If the default protection is not appropriate, you can customize the Firewall policy for each location, such as for a home site or customer site. If you do not want the default Firewall policy, you can edit it or replace it with another shared policy.

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

■ The default firewall protection blocks inbound and outbound IPv6 traffic with all remote systems.

Note: IPv6 is a network layer protocol that is used on the Internet. If you install the client on the computers that run Microsoft Vista, the **Rules** list includes several default rules that block the Ethernet protocol type of IPv6. If you remove the default rules, you must create a rule that blocks IPv6.

■ The default firewall protection restricts the inbound connections for a few protocols that are often used in attacks (for example, Windows file sharing). Internal network connections are allowed and external networks are blocked.

Table 20-2 describes the tasks that you can perform to configure a new firewall policy. You must add a firewall policy first, but thereafter, the remaining tasks are optional and you can complete them in any order.

Table 20-2   How to create a firewall policy

Task	Description
Add a firewall policy	When you create a new policy, you give it a name and a description. You also specify the groups to which the policy is applied.
	A firewall policy is automatically enabled when you create it. But you can disable if you need to.
	See "Enabling and disabling a firewall policy" on page 420.

Table 20-2 How to create a firewall policy *(continued)*

Task	Description
Create firewall rules	Firewall rules are the policy components that control how the firewall protects client computers from malicious incoming traffic and applications. The firewall automatically checks all incoming packets and outgoing packets against these rules. It allows or blocks the packets based on the information that is specified in rules. You can modify the default rules, create new rules, or disable the default rules.
	When you create a new Firewall policy, Symantec Endpoint Protection provides default firewall rules.
	The default firewall rules are enabled by default.
	See "Setting up firewall rules" on page 446.
Enable and customize notifications to users that access to an application is blocked	You can send users a notification that an application that they want to access is blocked.
	These settings are disabled by default.
	See "Notifying the users that access to an application is blocked" on page 439.
Enable automatic firewall rules	You can enable the options that automatically permit communication between certain network services. These options eliminate the need to create the rules that explicitly allow those services. You can also enable traffic settings to detect and block the traffic that communicates through NetBIOS and token rings.
	Only the traffic protocols are enabled by default.
	See "Automatically allowing communications for essential network services" on page 420.
	If the Symantec Endpoint Protection client detects a network attack, it can automatically block the connection to ensure that the client computer is safe. The client activates an Active Response, which automatically blocks all communication to and from the attacking computer for a set period of time. The IP address of the attacking computer is blocked for a single location.
	This option is disabled by default.
	See "Automatically blocking connections to an attacking computer" on page 422.

Table 20-2   How to create a firewall policy *(continued)*

Task	Description
Configure protection and stealth settings	You can enable settings to detect and log potential attacks on the client and block spoofing attempts. See "Detecting potential attacks and spoofing attempts" on page 423. You can enable the settings that prevent outside attacks from detecting information about your clients. See "Preventing stealth detection" on page 424. All of the protection options and stealth options are disabled by default.
Integrate the Symantec Endpoint Protection firewall with the Windows firewall	You can specify the conditions in which Symantec Endpoint Protection disables the Windows firewall. When Symantec Endpoint Protection is uninstalled, Symantec Endpoint Protection restores the Windows firewall setting to the state it was in before Symantec Endpoint Protection was installed. The default setting is to disable the Windows firewall once only and to disable the Windows firewall disabled message. See "Disabling the Windows firewall" on page 425.
Configure 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. **Note:** You can only view and enable this option if you install and license Symantec Network Access Control. This option is disabled by default. See "Configuring peer-to-peer authentication" on page 426.

See "Managing firewall protection" on page 413.

See "Best practices for Firewall policy settings" on page 260.

See "Editing a policy" on page 297.

Enabling and disabling a firewall policy

Firewall policies are automatically enabled when you create them. You can disable a firewall policy as needed, and then enable it again. You must enable a firewall policy for it to be active.

You might want to disable the firewall for any of the following reasons:

- You install an application that might cause the firewall to block it.

- A firewall rule or firewall setting blocks an application due to an administrator's mistake.

- The firewall causes network connectivity-related issues.

- The firewall might slow down the client computer.

You should enable at least the default firewall protection to keep your computers protected during remote client installation.

See "About enabling and disabling protection when you need to troubleshoot problems" on page 229.

To enable or disable a firewall policy

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

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

3 In the policy, on the **Overview** page, check **Enable this policy** to enable the policy; uncheck it to disable it.

4 Click **OK**.

See "Creating a firewall policy" on page 416.

See "Managing firewall protection" on page 413.

Automatically allowing communications for essential network services

You can enable the options that automatically permit communication between certain network services so you do not have to define the rules that explicitly allow those services. You can also enable traffic settings to detect and block the traffic that communicates through NetBIOS and token rings.

You can allow outbound requests and inbound replies for the network connections that are configured to use DHCP, DNS, and WINS traffic.

The filters allow DHCP, DNS, or WINS clients to receive an IP address from a server. It also protects the clients against attacks from the network with the following conditions:

| If the client sends a request to the server | The client waits for five seconds to allow an inbound response. |
| If the client does not send a request to the server | Each filter does not allow the packet. |

When you enable these options, Symantec Endpoint Protection permits the packet if a request was made; it does not block packets. You must create a firewall rule to block packets.

Note: To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

To automatically allow communications for essential network services

1   In the console, open a Firewall policy.

2   On the **Firewall Policy** page, click **Built-in Rules**.

3   Check the options that you want to enable.

4   Click **OK**.

5   If you are prompted, assign the policy to a location.

See "Creating a firewall policy" on page 416.

See "Editing a policy" on page 297.

See "Changing the user control level" on page 239.

Configuring firewall settings for mixed control

You can configure the client so that users have no control, full control, or limited control over which firewall settings they can configure.

Use the following guidelines when you configure the client:

Server control	The user cannot create any firewall rules or enable firewall settings.
Client control	The user can create firewall rules and enable all firewall settings.
Mixed control	The user can create firewall rules. You decide which firewall settings the user can enable.

To configure firewall settings for mixed control

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

2   Under **Clients**, select the group with the user control level that you want to modify.

3   On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.

4   To the right of **Client User Interface Control Settings**, click **Tasks > Edit Settings**.

5   In the **Control Mode Settings** dialog box, click **Mixed control**, and then click **Customize**.

6   On the **Client/Server Control Settings** tab, under the **Firewall Policy** category, do one of the following tasks:

   ■   To make a client setting available for the users to configure, click **Client**.

   ■   To configure a client setting, click **Server**.

7   Click **OK**.

8   Click **OK**.

9   For each firewall setting that you set to **Server**, enable or disable the setting in the Firewall policy.

See "Managing firewall protection" on page 413.

See "Automatically allowing communications for essential network services" on page 420.

See "Detecting potential attacks and spoofing attempts" on page 423.

See "Running commands on the client computer from the console" on page 233.

Automatically blocking connections to an attacking computer

If the Symantec Endpoint Protection client detects a network attack, it can automatically block the connection to ensure that the client computer is safe. The client activates an Active Response, which automatically blocks all communication to and from the attacking computer for a set period of time. The IP address of the attacking computer is blocked for a single location.

The attacker's IP address is recorded in the Security log. You can unblock an attack by canceling a specific IP address or canceling all Active Response.

If you set the client to mixed control, you can specify whether the setting is available on the client for the user to enable. If it is not available, you must enable it in the **Client User Interface Mixed Control Settings** dialog box.

Updated IPS signatures, updated denial-of-service signatures, port scans, and MAC spoofing also trigger an Active Response.

To automatically block connections to an attacking computer

1   In the console, open a Firewall policy.

2   On the **Firewall Policy** page in the left pane, click **Built-in Rules**.

3   Under **Other**, check **Automatically block an attacker's IP address**.

4   In the **Number of seconds during which to block IP address ... seconds** text box, specify the number of seconds to block potential attackers.

    You can enter a value from 1 to 999,999.

5   Click **OK**.

See "Creating a firewall policy" on page 416.

See "Configuring firewall settings for mixed control" on page 421.

See "Editing a policy" on page 297.

Detecting potential attacks and spoofing attempts

You can enable the various settings that enable Symantec Endpoint Protection to detect and log potential attacks on the client and block spoofing attempts. All of these options are disabled by default.

The settings that you can enable are as follows:

Enable port scan detection	When this setting is enabled, Symantec Endpoint Protection monitors all incoming packets that any security rule blocks. If a rule blocks several different packets on different ports in a short period of time, Symantec Endpoint Protection creates a Security log entry.
	Port scan detection does not block any packets. You must create a security policy to block traffic when a port scan occurs.
Enable denial of service detection	Denial of service detection is a type of intrusion detection. When enabled, the client blocks traffic if it detects a pattern from known signatures, regardless of the port number or type of Internet protocol.
Enable anti-MAC spoofing	When enabled, Symantec Endpoint Protection allows incoming and outgoing address resolution protocol (ARP) traffic if an ARP request was made to that specific host. All other unexpected ARP traffic is blocked and an entry is generated to the Security log.

Note: To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

To detect potential attacks and spoofing attempts

1   In the console, open a Firewall policy.

2   In the **Firewall Policy** page, click **Protection and Stealth**.

3   Under **Protection Settings**, check any of the options that you want to enable.

4   Click **OK**.

5   If you are prompted, assign the policy to a location.

See "Creating a firewall policy" on page 416.

See "Changing the user control level" on page 239.

See "Editing a policy" on page 297.

Preventing stealth detection

You can enable the settings that prevent outside attacks from detecting information about your clients. These settings are disabled by default.

Note: To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

To prevent stealth detection

1   In the console, open a Firewall policy.

2   In the **Firewall Policy** page, click **Protection and Stealth**.

3   Under **Stealth Settings**, check any of the options that you want to enable as follows:

Enable stealth mode Web browsing	Prevents the Web sites from knowing which operating system and browser your clients use.
Enable TCP resequencing	Randomizes the TCP sequencing number to evade operating system fingerprinting and some kinds of IP spoofing.
Enable OS fingerprint masquerading	Prevents the programs from detecting the operating system of the computer on which the firewall runs.

4 Click **OK**.

5 If you are prompted, assign the policy to a location.

Disabling the Windows firewall

You can specify the conditions in which Symantec Endpoint Protection disables the Windows firewall. When Symantec Endpoint Protection is uninstalled, Symantec Endpoint Protection restores the Windows firewall setting to the state it was in before Symantec Endpoint Protection was installed.

Note: Symantec Endpoint Protection does not modify any existing Windows firewall policy rules or exclusions.

The actions that Symantec Endpoint Protection can take are as follows:

No Action	Does not change the current Windows firewall setting.
Disable Once Only	Disables the Windows firewall at startup the first time Symantec Endpoint Protection detects that Windows firewall is enabled. On subsequent startups, Symantec Endpoint Protection does not disable the Windows firewall. This setting is the default.
Disable Always	Disables the Windows firewall at every startup and re-enables the Windows firewall if the Symantec Client Firewall is uninstalled.
Restore if Disabled	Enables the Windows firewall at startup.

Typically, a Windows user receives a notification when their computer restarts if the Windows firewall is disabled. Symantec Endpoint Protection disables this notification by default so that it does not alarm your users when the Windows firewall is disabled. But you can enable the notification, if desired.

To disable the Windows firewall

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

2 Under **Policies**, click **Firewall**.

3 Do one of the following tasks:

■ Create a new firewall policy.

■ In the **Firewall Policies** list, double-click on the firewall policy that you want to modify.

4   Under **Firewall Policy**, click **Windows Integration**.

5   In the **Disable Windows Firewall** drop-down list, specify when you want the Windows firewall disabled.

The default setting is Disable Once Only.

6   In the **Windows Firewall Disabled Message** drop-down list, specify whether you want to disable the Windows message on startup to indicate that the firewall is disabled.

The default setting is Disable, which means the user does not receive a message upon a computer startup that the Windows firewall is disabled.

7   Click **OK.**

See "Creating a firewall policy" on page 416.

See "The types of security policies" on page 293.

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.

Note: You must have Symantec Network Access Control is installed and licensed to view this option.

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 will 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 appears 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 that are 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 "Creating a firewall policy" on page 416.

See "Editing a policy" on page 297.

Managing firewall rules

Firewall rules control how the firewall protects computers from malicious incoming traffic and applications. The firewall checks all incoming packets and outgoing packets against the rules that you enable. It allows or blocks the packets based on the conditions that you specify in the firewall rule.

Symantec Endpoint Protection installs with a default firewall policy that contains default rules. When you create a new firewall policy, Symantec Endpoint Protection provides default firewall rules. You can modify any of the default rules or create new firewall rules if your administrator permits it, or if your client is unmanaged.

You must have at least one rule in a policy. But you can have as many rules as you need. You can enable or disable rules as needed. For example, you might want to disable a rule to perform troubleshooting and enable it when you are done.

Table 20-3 describes what you need to know to manage firewall rules.

Table 20-3   Managing firewall rules

Subject	Description
Learn how firewall rules work and what makes up a firewall rule	Before you modify the firewall rules, you should understand the following information about how firewall rules work. ■ The relationship between the client's user control level and the user's interaction with the firewall rules. The relationship between server rules and client rules. See "About firewall server rules and client rules" on page 429. ■ How to order rules to ensure that the most restrictive rules are evaluated first and the most general rules are evaluated last. See "About the firewall rule, firewall setting, and intrusion prevention processing order" on page 431. ■ The implications of inheriting rules from a parent group and how inherited rules are processed. See "About inherited firewall rules" on page 432. ■ That the client uses stateful inspection, which eliminates the need for you to create additional rules. See "How the firewall uses stateful inspection" on page 434. ■ The firewall components that make up the firewall rule. When you understand about these triggers and how you can best use them, you can customize your firewall rules to protect your clients and servers. See "About firewall rule application triggers" on page 435. See "About firewall rule host triggers" on page 440. See "About firewall rule network services triggers" on page 443. See "About firewall rule network adapter triggers" on page 445.

Table 20-3	Managing firewall rules *(continued)*
Subject	**Description**
Add a new firewall rule	You can perform the following tasks to manage firewall rules: ■ You can add new firewall rules through the console using several methods. One method lets you add a blank rule that has default settings. The other method offers a wizard that guides you through creating a new rule. See "Adding a new firewall rule" on page 447. ■ You can customize a default rule or one that you created by changing any of the firewall rule criteria. ■ Export and import firewall rules Another way that you can add a firewall rule is to export existing firewall rules from another Firewall policy. You can then import the firewall rules and settings so that you do not have to re-create them. See "Importing and exporting firewall rules" on page 448. ■ Copy and paste firewall rules You can save time creating a new firewall rule by copying an existing rule that is similar to the rule that you want to create. Then you can modify the copied rule to meet your needs. See "Copying and pasting firewall rules" on page 449.
Enable or disable a firewall rule	Firewall rules are automatically enabled. However, you may need to temporarily disable a firewall rule to test the rule. The firewall does not inspect disabled rules.
Customize a firewall rule	After you create a new rule, or if you want to customize a default rule, you can modify any of the firewall rule criteria. See "Customizing firewall rules" on page 450.

See "Managing firewall protection" on page 413.

About firewall server rules and client rules

Rules are categorized as either server rules or client rules. Server rules are the rules that you create in Symantec Endpoint Protection Manager and that are downloaded to the Symantec Endpoint Protection client. Client rules are the rules that the user creates on the client.

Table 20-4 describes the relationship between the client's user control level and the user's interaction with the firewall rules.

Table 20-4   User control level and rule status

User control level	User interaction
Server control	The client receives server rules but the user cannot view them. The user cannot create client rules.
Mixed control	The client receives server rules. The user can create client rules, which are merged with server rules and client security settings.
Client control	The client does not receive server rules. The user can create client rules. You cannot view client rules.

Table 20-5 lists the order that the firewall processes server rules, client rules, and client settings.

Table 20-5   Server rules and client rules processing priority

Priority	Rule type or setting
First	Server rules with high priority levels (rules above the blue line in the **Rules** list)
Second	Client rules
Third	Server rules with lower priority levels (rules under the blue line in the **Rules** list) On the client, server rules under the blue line are processed after client rules.
Fourth	Client security settings
Fifth	Client application-specific settings

On the client, users can modify a client rule or security setting, but users cannot modify a server rule.

Warning: If the client is in mixed control, users can create a client rule that allows all traffic. This rule overrides all server rules under the blue line.

See "Managing firewall rules" on page 428.

See "Changing the order of firewall rules" on page 434.

See "Changing the user control level" on page 239.

About the firewall rule, firewall setting, and intrusion prevention processing order

Firewall rules are ordered sequentially, from highest to lowest priority in the rules list. If the first rule does not specify how to handle a packet, the firewall inspects the second rule. This process continues until the firewall finds a match. After the firewall finds a match, the firewall takes the action that the rule specifies. Subsequent lower priority rules are not inspected. For example, if a rule that blocks all traffic is listed first, followed by a rule that allows all traffic, the client blocks all traffic.

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

The Rules list contains a blue dividing line. The dividing line sets the priority of rules in the following situations:

- When a subgroup inherits rules from a parent group.

- When the client is set to mixed control. The firewall processes both server rules and client rules.

Table 20-6 shows the order in which the firewall processes the rules, firewall settings, and intrusion prevention settings.

Table 20-6   Processing order

Priority	Setting
First	Custom IPS signatures
Second	Intrusion Prevention settings, traffic settings, and stealth settings
Third	Built-in rules
Fourth	Firewall rules
Fifth	Port scan checks
Sixth	IPS signatures that are downloaded through LiveUpdate

See "Changing the order of firewall rules" on page 434.

See "Managing firewall rules" on page 428.

See "How a firewall works" on page 415.

See "How intrusion prevention works" on page 464.

About inherited firewall rules

A subgroup's policy can inherit only the firewall rules that are enabled in the parent group. When you have inherited the rules, you can disable them, but you cannot modify them. As the new rules are added to the parent group's policy, the new rules are automatically added to the inheriting policy.

When the inherited rules appear in the **Rules** list, they are shaded in purple. Above the blue line, the inherited rules are added above the rules that you created. Below the blue line, the inherited rules are added below the rules that you created.

A Firewall policy also inherits default rules, so the subgroup's Firewall policy may have two sets of default rules. You may want to delete one set of default rules.

If you want to remove the inherited rules, you remove the inheritance rather than delete them. You have to remove all the inherited rules rather than the selected rules.

The firewall processes inherited firewall rules in the **Rules** list as follows:

Above the blue dividing line	The rules that the policy inherits take precedence over the rules that you create.
Below the blue dividing line	The rules that you create take precedence over the rules that the policy inherits.

Figure 20-1 shows how the **Rules** list orders rules when a subgroup inherits rules from a parent group. In this example, the Sales group is the parent group. The Europe Sales group inherits from the Sales group.

Figure 20-1   An example of how firewall rules inherit from each other
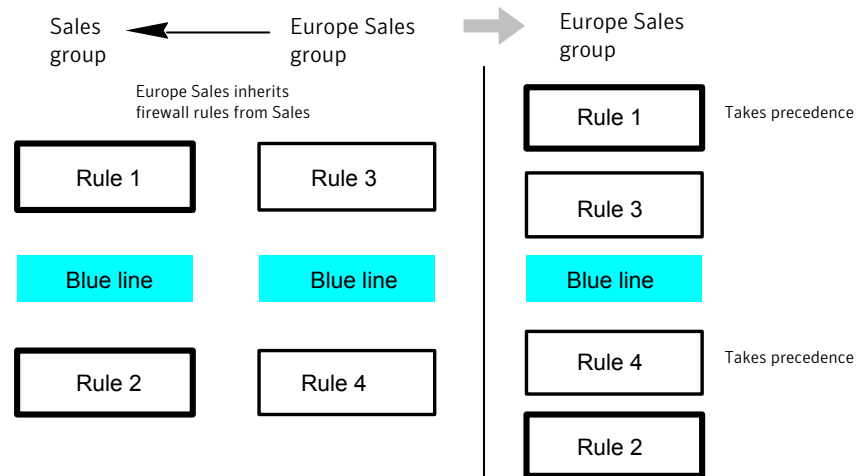
See "Managing firewall rules" on page 428.

See "Adding inherited firewall rules from a parent group" on page 433.

Adding inherited firewall rules from a parent group

You can add firewall rules to a firewall policy by inheriting rules from a parent group. To inherit the rules from a parent group, the subgroup's policy must be a non-shared policy.

Note: If the group inherits all of its policies from a parent group, this option is unavailable.

To add inherited firewall rules from a parent group

1   In the console, open a Firewall policy.

2   On the **Firewall Policy** page, click **Rules**.

3   On the **Rules** tab, check **Inherit Firewall Rules from Parent Group**.

     To remove the inherited rules, uncheck **Inherit Firewall Rules from Parent Group**.

4   Click **OK**.

See "Editing a policy" on page 297.

See "About inherited firewall rules" on page 432.

See

Changing the order of firewall rules

The firewall processes the list of firewall rules from the top down. You can determine how the firewall processes firewall rules by changing their order.

When you change the order, it affects the order for the currently selected location only.

Note: For better protection, place the most restrictive rules first and the least restrictive rules last.

To change the order of firewall rules

1   In the console, open a Firewall policy.

2   In the **Firewall Policy** page, click **Rules**, and then select the rule that you want to move.

3   Do one of the following tasks:

   ■   To process this rule before the previous rule, click **Move Up**.

   ■   To process this rule after the rule below it, click **Move Down**.

4   Click **OK**.

See

See

See

How the firewall uses stateful inspection

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

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

Stateful inspection eliminates the need to create new rules. For the traffic that is initiated in one direction, you do not have to create the rules that permit the traffic in both directions. The client traffic that is initiated in one direction includes Telnet (port 23), HTTP (port 80), and HTTPS (port 443). The client computers initiate this outbound traffic; you create a rule that permits the outbound traffic for these protocols. Stateful inspection automatically permits the return traffic that responds to the outbound traffic. Because the firewall is stateful in nature, you only need to create the rules that initiate a connection, not the characteristics of a particular packet. All packets that belong to an allowed connection are implicitly allowed as being an integral part of that same connection.

Stateful inspection supports all rules that direct TCP traffic.

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

See "How a firewall works" on page 415.

See "Managing firewall rules" on page 428.

About firewall rule application triggers

When the application is the only trigger you define in a rule that allows traffic, the firewall allows the application to perform any network operation. The application is the significant value, not the network operations that the application performs. For example, suppose you allow Internet Explorer and you define no other triggers. Users can access the remote sites that use HTTP, HTTPS, FTP, Gopher, and any other protocol that the Web browser supports. You can define additional triggers to describe the particular network protocols and hosts with which communication is allowed.

Application-based rules may be difficult to troubleshoot because an application may use multiple protocols. For example, if the firewall processes a rule that allows Internet Explorer before a rule that blocks FTP, the user can still communicate with FTP. The user can enter an FTP-based URL in the browser, such as ftp://ftp.symantec.com.

For example, suppose you allow Internet Explorer and define no other triggers. Computer users can access the remote sites that use HTTP, HTTPS, FTP, Gopher, and any other protocol that the Web browser supports. You can define additional triggers to describe the network protocols and hosts with which communication is allowed.

You should not use application rules to control traffic at the network level. For example, a rule that blocks or limits the use of Internet Explorer would have no

effect should the user use a different Web browser. The traffic that the other Web browser generates would be compared against all other rules except the Internet Explorer rule. Application-based rules are more effective when the rules are configured to block the applications that send and receive traffic.

See "Defining information about applications" on page 436.

See "Notifying the users that access to an application is blocked" on page 439.

See "Managing firewall rules" on page 428.

See "Blocking networked applications that might be under attack" on page 437.

Defining information about applications

You can define information about the applications that clients run and include this information in a firewall rule.

You can define applications in the following ways:

- Type the information manually.
  See "To define information about applications manually" on page 436.

- Search for the application in the learned applications list.
  Applications in the learned applications list are the applications that client computers in your network run.
  See "To search for applications from the learned applications list" on page 437.

To define information about applications manually

1 In the console, open a Firewall policy.

2 On the **Firewall Policies** page, click **Rules**.

3 On the **Rules** tab, in the **Rules** list, right-click the **Application** field, and then click **Edit**.

4 In the **Application List** dialog box, click **Add**.

5 In the **Add Application** dialog box, enter one or more of the following fields:

    - Path and file name

    - Description

    - Size, in bytes

    - Date that the application was last changed

    - File fingerprint

6 Click **OK**.

7 Click **OK**.

To search for applications from the learned applications list

1   On the **Firewall Policies** page, click **Rules**.

2   On the **Rules** tab, select a rule, right-click the **Application** field, and then click **Edit**.

3   In the **Application List** dialog box, click **Add From**.

4   In the **Search for Applications** dialog box, search for an application.

5   Under the **Query Results** table, to add the application to the **Applications** list, select the application, click **Add**, and then click **OK**.

6   Click **Close**.

7   Click **OK**.

See "Managing firewall rules" on page 428.

See "Editing a policy" on page 297.

See "About firewall rule application triggers" on page 435.

Blocking networked applications that might be under attack

Network application monitoring tracks an application's behavior in the security log. If an application's content is modified too frequently, it is likely that a Trojan horse attacked the application and the client computer is not safe. If an application's content is modified on an infrequent basis, it is likely that a patch was installed and the client computer is safe. You can use this information to create a firewall rule that allows or blocks an application.

You can configure the client to detect and monitor any application that runs on the client computer and that is networked. Network applications send and receive traffic. The client detects whether an application's content changes.

If you suspect that a Trojan horse has attacked an application, you can use network application monitoring to configure the client to block the application. You can also configure the client to ask users whether to allow or block the application.

An application's content changes for the following reasons:

■   A Trojan horse attacked the application.

■   The application was updated with a new version or an update.

You can add applications to a list so that the client does not monitor them. You may want to exclude the applications that you think are safe from a Trojan horse attack, but that have frequent and automatic patch updates.

You may want to disable network application monitoring if you are confident that the client computers receive adequate protection from antivirus and antispyware

protection. You may also want to minimize the number of notifications that ask users to allow or block a network application.

To block networked applications that might be under attack

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

2   Under **Clients**, select a group, and then click **Policies**.

3   On the **Policies** tab, under **Location-independent Policies and Settings**, click **Network Application Monitoring**.

4   In the **Network Application Monitoring for** *group name* dialog box, click **Enable Network Application Monitoring**.

5   In the **When an application change is detected** drop-down list, select the action that the firewall takes on the application that runs on the client as follows:

Ask	Asks the user to allow or block the application.
Block the traffic	Blocks the application from running.
Allow and Log	Allows the application to run and records the information in the security log.
	The firewall takes this action on the applications that have been modified only.

6   If you selected **Ask**, click **Additional Text**.

7   In the **Additional Text** dialog box, type the text that you want to appear under the standard message, and then click **OK**.

8   To exclude an application from being monitored, under **Unmonitored Application List**, do one of the following tasks:

To define an application manually	Click **Add**, fill out one or more fields, and then click **OK**.
To define an application from a learned applications list	Click **Add From**. The learned applications list monitors both networked and non-networked applications. You must select networked applications only from the learned applications list. After you have added applications to the **Unmonitored Applications List**, you can enable, disable, edit, or delete them.

9 Check the box beside the application to enable it; uncheck it to disable it.

10 Click **OK**.

See "Managing firewall rules" on page 428.

See "Notifying the users that access to an application is blocked" on page 439.

See "About firewall rule application triggers" on page 435.

See "Searching for information about the applications that the computers run" on page 314.

See "Configuring the management server to collect information about the applications that the client computers run" on page 313.

Notifying the users that access to an application is blocked

You can send users a notification that an application that they want to access is blocked. This notification appears on the users' computers.

Note: Enabling too many notifications can not only overwhelm your users, but can also alarm them. Use caution when enabling notifications.

To notify the users that access to an application is blocked

1 In the console, open a Firewall policy.

2 On the **Firewall Policies** page, click **Rules**.

3 On the **Notifications** tab, check the following options that you want to apply:

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

4 Click **OK**.

See "Managing firewall protection" on page 413.

See "Enabling and disabling a firewall policy" on page 420.

See "Managing firewall rules" on page 428.

See "About firewall rule application triggers" on page 435.

See "Blocking networked applications that might be under attack" on page 437.

About firewall rule host triggers

You specify the host on both sides of the described network connection when you define host triggers.

Traditionally, the way to express the relationship between hosts is referred to as being either the source or destination of a network connection.

You can define the host relationship in either one of the following ways:

Source and destination	The source host and destination host is dependent on the direction of traffic. In one case the local client computer might be the source, whereas in another case the remote computer might be the source.
	The source and the destination relationship are more commonly used in network-based firewalls.
Local and remote	The local host is always the local client computer, and the remote host is always a remote computer that is positioned elsewhere on the network. This expression of the host relationship is independent of the direction of traffic.
	The local and the remote relationship is more commonly used in host-based firewalls, and is a simpler way to look at traffic.

You can define multiple source hosts and multiple destination hosts.

Figure 20-2 illustrates the source relationship and destination relationship with respect to the direction of traffic.

Figure 20-2   The relationship between source and destination hosts
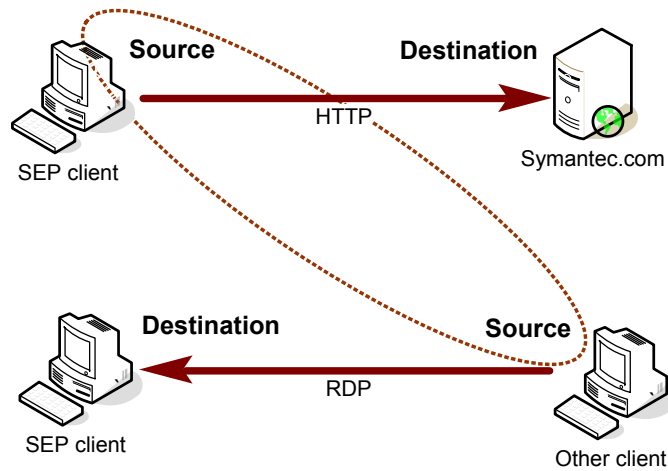
Figure 20-3 illustrates the local host and remote host relationship with respect to the direction of traffic.

Figure 20-3   The relationship between local and remote hosts
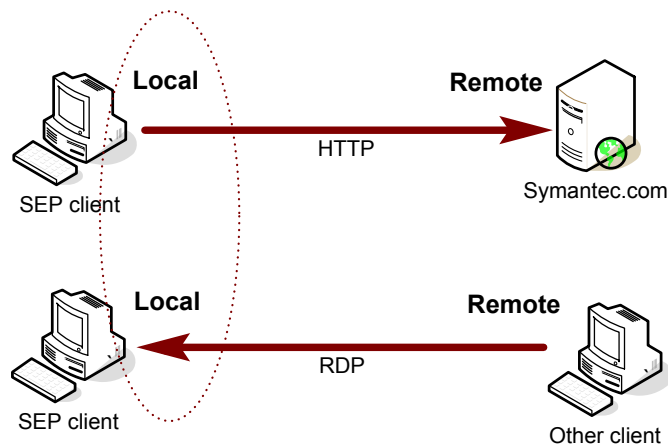
Relationships are evaluated by the following types of statements:

The hosts that you define on either side of the connection (between the source and the destination)	OR statement
Selected hosts	AND statement

For example, consider a rule that defines a single local host and multiple remote hosts. As the firewall examines the packets, the local host must match the relevant IP address. However, the opposing sides of the address may be matched to any remote host. For example, you can define a rule to allow HTTP communication between the local host and either Symantec.com, Yahoo.com, or Google.com. The single rule is the same as three rules.

See "Adding host groups" on page 442.

See "Blocking traffic to or from a specific server" on page 453.

See "Managing firewall rules" on page 428.

Adding host groups

A host group is a collection of: DNS domain names, DNS host names, IP addresses, IP ranges, MAC addresses, or subnets that are grouped under one name. The purpose of host groups is to eliminate the retyping of host addresses and names. For example, you can add multiple IP addresses one at a time to a firewall rule. Or, you can add multiple IP addresses to a host group, and then add the group to the firewall rule.

As you incorporate host groups, you must describe where the groups are used. If you decide later to delete a host group, you must first remove the host group from all the firewall rules that reference the group.

When you add a host group, it appears at the bottom of the **Hosts** list. You can access the **Hosts** list from the **Host** field in a firewall rule.

To add host groups

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

2 Expand **Policy Components**, and then click **Host Groups**.

3 Under **Tasks**, click **Add a Host Group**.

4 In the **Host Group** dialog box, type a name, and then click **Add**.

5 In the **Host** dialog box, in the **Type** drop-down list, select a host.

6 Type the appropriate information for each host type.

7 Click **OK**.

8 Add additional hosts, if necessary.

9 Click **OK**.

See "About firewall rule host triggers" on page 440.

Defining DNS queries based on location

You can define how frequently you want a specific location to perform a DNS query. This feature lets you configure one location to query the DNS server more often than other locations.

For example, assume that you have a policy to block all traffic outside of your corporate network except VPN traffic. And assume that your users travel and must access your network through a VPN from a hotel network. You can create a policy for a VPN connection that uses DNS resolution. Symantec Endpoint Protection continues to send the DNS query every 5 seconds until it switches to this location. This way, your users can more quickly access your network.

Caution: Use caution when you configure this setting to a very low value. You run the possibility of bringing down your DNS server if all of your systems access the server every 5 seconds, for example.

To define DNS queries based on location

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

2   Under **Clients**, select the group for which the feature applies.

3   Under **Tasks**, click **Manage Locations**.

4   Ensure **DNS Query Loop in** is checked.

5   Click the time setting and increments and modify as desired.

    You can set the value in seconds, minutes, or hours.

    The default value is 30 minutes.

6   Click **OK**.

See "Managing firewall rules" on page 428.

See "About firewall rule host triggers" on page 440.

About firewall rule network services triggers

Network services let networked computers send and receive messages, share files, and print. A network service uses one or more protocols or ports to pass through a specific type of traffic. For example, the HTTP service uses ports 80 and 443 in the TCP protocol. You can create a firewall rule that allows or blocks network services. A network service trigger identifies one or more network protocols that are significant in relation to the described network traffic.

When you define TCP-based or UDP-based service triggers, you identify the ports on both sides of the described network connection. Traditionally, ports are referred to as being either the source or the destination of a network connection.

See "Adding network services to the default network services list" on page 444.

See "Permitting clients to browse for files and printers in the network" on page 455.

See "Managing firewall rules" on page 428.

Adding network services to the default network services list

Network services let networked computers send and receive messages, share files, and print. You can create a firewall rule that allows or blocks network services.

The network services list eliminates the need to retype protocols and ports for the firewall rules that you create to block or allow network services. When you create a firewall rule, you can select a network service from a default list of commonly used network services. You can also add network services to the default list. However, you need to be familiar with the type of protocol and the ports that it uses.

Note: IPv4 and IPv6 are the two network layer protocols that are used on the Internet. The firewall blocks the attacks that travel through IPv4, but not through IPv6. If you install the client on the computers that run Microsoft Vista, the **Rules** list includes several default rules that block the Ethernet protocol type of IPv6. If you remove the default rules, you must create a rule that blocks IPv6.

Note: You can add a custom network service through a firewall rule. However, that network service is not added to the default list. You cannot access the custom network service from any other rule.

To add network services to the default network services list

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

2   Expand **Policy Components**, and then click **Network Services**.

3   Under **Tasks**, click **Add a Network Service**.

4   In the **Network Service** dialog box, type a name for the service, and then click **Add**.

5   Select a protocol from the **Protocol** drop-down list.

    The options change based on which protocol you select.

6   Type in the appropriate fields, and then click **OK**.

7 Add one or more additional protocols, as necessary.

8 Click **OK**.

See "Managing firewall rules" on page 428.

See "About firewall rule network services triggers" on page 443.

See "Controlling whether networked computers can share messages, files, and printing" on page 455.

See "Permitting clients to browse for files and printers in the network" on page 455.

About firewall rule network adapter triggers

You can define a firewall rule that blocks or allows traffic that passes through (transmitted or received) a network adapter.

When you define a particular type of adapter, consider how that adapter is used. For example, if a rule allows outbound HTTP traffic from Ethernet adapters, then HTTP is allowed through all the installed adapters of the same type. The only exception is if you also specify local host addresses. The client computer may use multi-NIC servers and the workstations that bridge two or more network segments. To control traffic relative to a particular adapter, the address scheme of each segment must be used rather than the adapter itself.

The network adapter list eliminates the need to retype types of adapters for firewall rules. Instead, when you create a firewall rule, you can select a network adapter from a default list of commonly used network adapters. You can also add network adapters to the default list.

You can select a network adapter from a default list that is shared across firewall policies and rules. The most common adapters are included in the default list in the **Policy Components** list. The common adapters include VPNs, Ethernet, wireless, Cisco, Nortel, and Enterasys adapters.

Note: You can add a custom network adapter through a firewall rule. However, that network adapter is not added to the default list. You cannot access the custom network adapter from any other rule.

See "Managing firewall rules" on page 428.

See "Adding a custom network adapter to the network adapter list" on page 446.

See "Controlling the traffic that passes through a network adapter" on page 458.

Adding a custom network adapter to the network adapter list

You can apply a separate firewall rule to each network adapter. For example, you may want to block traffic through a VPN at an office location, but not at a home location.

You can select a network adapter from a default list that is shared across firewall policies and rules. The most common adapters are included in the default list in the **Policy Components** list. Use the default list so that you do not have to retype each network adapter for every rule that you create.

The network adapter list eliminates the need to retype adapters for firewall rules. When you create a firewall rule, you can select a network adapter from a default list of commonly used network adapters. You can also add network adapters to the default list.

Note: You can add a custom network adapter through a firewall rule. However, that network adapter is not added to the default list. You cannot access the custom network adapter from any other rule.

To add a custom network adapter to the network adapter list

1 In the console, click **Policies > Policy Components > Network Adapters**.

2 Under **Tasks**, click **Add a Network Adapter**.

3 In the **Network Adapter** dialog box, in the **Adapter Type** drop-down list, select an adapter.

4 In the **Adapter Name** field, optionally type a description.

5 In the **Adapter Identification** text box, type the case-sensitive brand name of the adapter.

   To find the brand name of the adapter, open a command line on the client, and then type the following text:

   ```
   ipconfig/all
   ```

6 Click **OK**.

See "Managing firewall rules" on page 428.

See "About firewall rule network adapter triggers" on page 445.

See "Controlling the traffic that passes through a network adapter" on page 458.

Setting up firewall rules

Table 20-7 describes how to set up new firewall rules.

Table 20-7   How to setup firewall rules

Step	Task	Description
Step 1	Add a new firewall rule	You can add new firewall rules through the console using several methods. One method lets you add a blank rule that has default settings. The other method offers a wizard that guides you through creating a new rule. See "Adding a new firewall rule" on page 447. Another way that you can add a firewall rule is to export existing firewall rules from another Firewall policy. You can then import the firewall rules and settings so that you do not have to re-create them. See "Importing and exporting firewall rules" on page 448. You can save time creating a new firewall rule by copying an existing rule that is similar to the rule that you want to create. Then you can modify the copied rule to meet your needs. See "Copying and pasting firewall rules" on page 449.
Step 2	(Optional) Customize the firewall rule criteria	After you create a new rule, or if you want to customize a default rule, you can modify any of the firewall rule criteria. See "Customizing firewall rules" on page 450.

See "Managing firewall rules" on page 428.

Adding a new firewall rule

You can create new firewall rules using either of the following methods:

Blank rule

A blank rule allows all traffic.

See "To add a new blank firewall rule" on page 448.

Add Firewall Rule wizard

If you add rules with the **Add Firewall Rule** wizard, ensure that you configure the rule. The wizard does not configure new rules with multiple criteria.

See "To add a new firewall rule using a wizard" on page 448.

You should specify both the inbound and the outbound traffic in the rule whenever possible. You do not need to create inbound rules for traffic such as HTTP. The Symantec Endpoint Protection client uses stateful inspection for TCP traffic. Therefore, it does not need a rule to filter the return traffic that the clients initiate.

When you create a new firewall rule, it is automatically enabled. You can disable a firewall rule if you need to allow specific access to a computer or application. The rule is disabled for all inherited policies.

The rule is also disabled for the all locations if it is a shared policy, and only one location if it is a location-specific policy.

Note: Rules must be enabled for the firewall to process them.

To add a new blank firewall rule

1   In the console, open a Firewall policy.

2   On the **Firewall Policy** page, click **Rules**.

3   On the **Rules** tab, under the **Rules** list, click **Add Blank Rule**.

4   Optionally, you can customize the firewall rule criteria as needed.

5   If you are done with the configuration of the rule, click **OK**.

To add a new firewall rule using a wizard

1   In the console, open a Firewall policy.

2   On the **Firewall Policy** page, click **Rules**.

3   On the **Rules** tab, under the **Rules** list, click **Add Rule**.

4   In the **Add Firewall Rule Wizard**, click **Next**.

5   In the **Select Rule Type** panel, select one of the types of rules.

6   Click **Next**.

7   Enter data on each panel to create the type of rule you selected.

8   For applications and hosts, click **Add More** to add additional applications and services.

9   When you are done, click **Finish**.

10 Optionally, you can customize the firewall rule criteria as needed.

11 If you are done with the configuration of the rule, click **OK**.

See "Customizing firewall rules" on page 450.

See "Setting up firewall rules" on page 446.

See "Editing a policy" on page 297.

See "How the firewall uses stateful inspection" on page 434.

Importing and exporting firewall rules

You can export and import firewall rules and settings from another Firewall policy so that you do not have to re-create them. For example, you can import a partial

rule set from one policy into another. To import rules, you first have to export
the rules to a .dat file and have access to the file.

The rules are added in the same order that they are listed in the parent policy
with respect to the blue line. You can then change their processing order.

To export firewall rules

1   In the console, open a Firewall policy.

2   On the **Firewall Policy** page, click **Rules**.

3   In the **Rules** list, select the rules you want to export, right-click, and then
    click **Export**.

4   In the **Export Policy** dialog box, locate a directory to save the .dat file, type
    a file name, and then click **Export**.

To import firewall rules

1   In the console, open a Firewall policy.

2   On the **Firewall Policy** page, click **Rules**.

3   Right-click the Rules list, and then click **Import**.

4   In the **Import Policy** dialog box, locate the .dat file that contains the firewall
    rules to import, and then click **Import**.

5   In the **Input** dialog box, type a new name for the policy, and then click **OK**.

6   Click **OK**.

See "Setting up firewall rules" on page 446.

See "Customizing firewall rules" on page 450.

See "About the firewall rule, firewall setting, and intrusion prevention processing
order" on page 431.

See "Editing a policy" on page 297.

Copying and pasting firewall rules

Save time creating a new firewall rule by copying an existing rule that is similar
to the new rule that you want to create. Then you can modify the copied rule as
needed.

You can copy and paste rules from the same policy or another policy.

To copy and paste firewall rules

1   In the console, open a Firewall policy.

2   In the **Firewall Policy** page, click **Rules**.

3 On the **Rules** tab, right-click the rule you want to copy, and then click **Copy Rule**.

4 Right-click the row where you want the rule to be pasted, and then click **Paste Rule**.

5 Click **OK**.

See "Customizing firewall rules" on page 450.

See "Setting up firewall rules" on page 446.

See "Editing a policy" on page 297.

Customizing firewall rules

When you create a new Firewall policy, the policy includes several default rules. You can modify one or multiple rule components as needed.

The components of a firewall rule are as follows:

Actions   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.

The actions are as follows:

■ Allow
  The firewall allows the network connection.
■ Block
  The firewall blocks the network connection.

Triggers	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.

The triggers are as follows:

- Application
  When the application is the only trigger you define in an allow-traffic rule, the firewall allows the application to perform any network operation. The application is the significant value, not the network operations that the application performs. You can define additional triggers to describe the particular network protocols and hosts with which communication is allowed.
  See "About firewall rule application triggers" on page 435.
- Host
  When you define host triggers, you specify the host on both sides of the described network connection.
  Traditionally, the way to express the relationship between hosts is referred to as being either the source or destination of a network connection.
  See "About firewall rule host triggers" on page 440.
- Network services
  A network services trigger identifies one or more network protocols that are significant in relation to the described traffic.
  The local host computer always owns the local port, and the remote computer always owns the remote port. This expression of the port relationship is independent of the direction of traffic.
  See "About firewall rule network services triggers" on page 443.
- Network adapter
  If you define a network adapter trigger, the rule is relevant only to the traffic that is transmitted or received by using the specified type of adapter. You can specify either any adapter or the one that is currently associated with the client computer.
  See "About firewall rule network adapter triggers" on page 445.

Conditions	Rule conditions consist of the rule 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.

Notifications   The Log settings let you specify whether the server creates a log entry or sends an email message when a traffic event matches the criteria that are set for this rule.

The Severity setting lets you specify the severity level of the rule violation.

Customizing firewall rules

1   In the console, open a Firewall policy.

2   On the **Firewall Policy** page, click **Rules**.

3   On the **Rules** tab, in the **Rules** list, in the **Enabled** field, ensure that the box is checked to enable the rule; uncheck the box to disable the rule.

Symantec Endpoint Protection only processes the rules that you enable. All rules are enabled by default.

4   Double-click the **Name** field and type a unique name for the firewall rule.

5   Right-click the **Action** field and select the action that you want Symantec Endpoint Protection to take if the rule is triggered.

6   In the **Application** field, define an application.

See "Defining information about applications" on page 436.

7   In the **Host** field, specify a host trigger.

See "Blocking traffic to or from a specific server" on page 453.

8   In addition to specifying a host trigger, you can also specify the traffic that is allowed to access your local subnet.

See "Allowing only specific traffic to the local subnet" on page 454.

9   In the **Service** field, specify a network service trigger.

See "Controlling whether networked computers can share messages, files, and printing" on page 455.

10 In the **Log** field, specify when you want Symantec Endpoint Protection to send an email message to you when this firewall rule is violated.

See "Setting up notifications for firewall rule violations" on page 457.

11 Right-click the **Severity** field and select the severity level for the rule violation.

12 In the **Adapter** column, specify an adapter trigger for the rule.

See "Controlling the traffic that passes through a network adapter" on page 458.

13 In the **Time** column, specify the time periods in which this rule is active.

See "Scheduling when a firewall rule is active" on page 459.

14 Right-click the **Screen Saver** field and specify the state that the client computer's screen saver must be in for the rule to be active.

The **Created At** field is not editable. If the policy is shared, the term Shared appears. If the policy is not shared, the field shows the name of the group to which that the non-shared policy is assigned.

15 Right-click the **Description** field, click **Edit**, type an optional description for the rule, and then click **OK**.

16 If you are done with the configuration of the rule, click **OK**.

See "Setting up firewall rules" on page 446.

See "Managing firewall rules" on page 428.

Blocking traffic to or from a specific server

To block traffic to or from a specific server, you can block the traffic by IP address rather than by domain name or host name. Otherwise, the user may be able to access the IP address equivalent of the host name.

To block traffic to or from a specific server

1 In the console, open a Firewall policy.

2 On the **Firewall Policy** page, click **Rules**.

3 On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Host** field, and then click **Edit**.

4 In the **Host List** dialog box, do one of the following actions:

- Click **Source/Destination**.

- Click **Local/Remote**.

5 Do one of the following tasks:

To select a host type from the **Type** drop-down list	Do all of the following tasks: ■ In the **Source and Destination or Local and Remote** tables, click **Add**. ■ In the **Host dialog** box, select a host type from the **Type** drop-down list, and type the appropriate information for each host type. ■ Click **OK**. The host that you created is automatically enabled.

To select a host group	In the **Host List** dialog box, do one of the following actions:
	■ Click **Source/Destination**.
	■ Click **Local/Remote**.
	Then in the **Host List** dialog box, check the box in the **Enabled** column for any host group that you want to added to the rule.

6   Add additional hosts, if necessary.

7   Click **OK** to return to the **Rules** list.

See "Setting up firewall rules" on page 446.

See "Customizing firewall rules" on page 450.

See "Editing a policy" on page 297.

See "Adding host groups" on page 442.

Allowing only specific traffic to the local subnet

You can create a firewall rule that permits only specific traffic to your local subnet. This firewall rule always applies to your local subnet IP address, regardless of what the address is. Therefore, even if you change your local subnet IP address, you never have to modify this rule for the new address.

For example, you can create this rule to permit traffic to port 80 only on the local subnet, regardless of what the local subnet IP address is.

To allow only specific traffic to the local subnet

1   In the console, open a Firewall policy.

2   On the **Firewall Policy** page, click **Rules**.

3   On the **Rules** tab, in the **Rules** list, select the rule that you want to edit.

4   In the **Firewall Rules** table, in the **Host** column, double-click on the rule for which you want to create a local subnet traffic condition.

5   Under the type of hosts for which this rule applies (Local or Remote), click **Add**.

6   Click the **Address Type** drop-down list and select **Local Subnet**.

7   Click **OK**, and then click **OK** again to close out of the **Host List** dialog box.

See "The types of security policies" on page 293.

See "Editing a policy" on page 297.

See "Customizing firewall rules" on page 450.

Controlling whether networked computers can share messages, files, and printing

Network services let networked computers send and receive messages, shared files, and print. You can create a firewall rule that allows or blocks network services.

You can add a custom network service through a firewall rule. However, that network service is not added to the default list. You cannot access the custom service from any other rule.

To control whether networked computers can share messages, files, and printing

1   In the console, open a Firewall policy.

2   On the **Firewall Policy** page, click **Rules**.

3   On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Service** field, and then click **Edit**.

4   In the **Service List** dialog box, check box beside each service that you want to trigger the rule.

5   To add an additional service for the selected rule only, click **Add**.

6   In the **Protocol** dialog box, select a protocol from the **Protocol** drop-down list.

7   Fill out the appropriate fields.

8   Click **OK**.

9   Click **OK**.

10 Click **OK**.

See "About firewall rule network services triggers" on page 443.

See "Setting up firewall rules" on page 446.

See "Adding network services to the default network services list" on page 444.

See "Editing a policy" on page 297.

See "Customizing firewall rules" on page 450.

Permitting clients to browse for files and printers in the network

You can enable the client to either share its files or to browse for shared files and printers on the local network. To prevent network-based attacks, you may not want to enable network file and printer sharing.

You enable network file and print sharing by adding firewall rules. The firewall rules allow access to the ports to browse and share files and printers. You create one firewall rule so that the client can share its files. You create a second firewall rule so that the client can browse for other files and printers.

The settings work differently based on the type of control that you specify for your client, as follows:

Client control or mixed control	Users on the client can enable these settings automatically by configuring them in Network Threat Protection.
Mixed control	A server firewall rule that specifies this type of traffic can override these settings.
Server control	These settings are not available on the client.

To permit clients to browse for files and printers in the network

1   In the console, open a Firewall policy.

2   On the **Firewall Policy** page, click **Rules**.

3   On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Service** field, and then click **Edit**.

4   In the **Service List** dialog box, click **Add**.

5   In the **Protocol** dialog box, in the **Protocol** drop-down list, click **TCP**, and then click **Local/Remote**.

6   Do one of the following tasks:

To permit clients to browse for files and printers in the network	In the **Remote port** drop-down list, type **88, 135, 139, 445**.
To enable other computers to browse files on the client	In the **Local Port** drop-down list, type **88, 135, 139, 445**.

7   Click **OK**.

8   In the **Service List** dialog box, click **Add**.

9   In the **Protocol** dialog box, in the **Protocol** drop-down list, click **UDP**.

10 Do one of the following tasks:

To permit clients to browse for files and printers in the network	In the **Local Port** drop-down list, type **137, 138**. In the **Remote Port** drop-down list, type **88**.
To enable other computers to browse files on the client	In the **Local Port** drop-down list, type **88, 137, 138**.

11 Click **OK**.

12 In the **Service List** dialog box, make sure that the two services are enabled, and then click **OK**.

13 On the **Rules** tab, make sure the **Action** field is set to **Allow**.

14 If you are done with the configuration of the policy, click **OK**.

15 If you are prompted, assign the policy to a location.

See "Setting up firewall rules" on page 446.

See "Customizing firewall rules" on page 450.

See "Editing a policy" on page 297.

Setting up notifications for firewall rule violations

You can configure Symantec Endpoint Protection to send you an email message each time the firewall detects a rule violation, attack, or event. For example, you may want to know when a client blocks the traffic that comes from a particular IP address.

To set up notifications for firewall rule violations

1 In the console, open a Firewall policy.

2 On the **Firewall Policy** page, click **Rules**.

3 On the **Rules** tab, select a rule, right-click the **Logging** field, and do one or more of the following tasks:

To send an email message when a firewall rule is triggered	Check **Send Email Alert**.
To generate a log event when a firewall rule is triggered	Check both **Write to Traffic Log** and **Write to Packet Log**.

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

5   Configure a security alert.

6   Configure a mail server.

7   Click **OK**.

See "Setting up firewall rules" on page 446.

See "Customizing firewall rules" on page 450.

See "Setting up administrator notifications" on page 642.

Controlling the traffic that passes through a network adapter

When you define a network adapter trigger, the rule is relevant only to the traffic that the specified adapter transmits or receives.

You can add a custom network adapter from a firewall rule. However, that adapter is not added to the shared list. You cannot access the custom adapter from any other rule.

To control the traffic that passes through a network adapter

1   In the console, open a Firewall policy.

2   On the **Firewall Policy** page, click **Rules**.

3   On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Adapter** field, and then click **More Adapters**.

4   In the **Network Adapter** dialog box, do one of the following actions:

To trigger the rule for any adapter (even if it is not listed)	Click **Apply the rule to all adapters**, and then go to step 7.
To trigger the rule for selected adapters	Click **Apply the rule to the following adapters**.
	Then check the box beside each adapter that you want to trigger the rule.

5   To add a custom adapter for the selected rule only, do the following tasks:

  ■ Click **Add**.

  ■ In the **Network Adapter** dialog box, select the adapter type and type the adapter's brand name in the **Adapter Identification** text field.

6   Click **OK**.

7 Click **OK**.

8 Click **OK**.

See "Setting up firewall rules" on page 446.

See "Customizing firewall rules" on page 450.

See "Editing a policy" on page 297.

See "About firewall rule network adapter triggers" on page 445.

Scheduling when a firewall rule is active

You can specify a time period when a firewall rule is active.

To schedule when a firewall rule is active

1 In the console, open a Firewall policy.

2 On the **Firewall Policy** page, click **Rules**.

3 On the **Rules** tab, select the rule you want to edit, right-click the **Time** field, and then click **Edit**.

4 In the **Schedule List** dialog box, click **Add**.

5 In the **Add Schedule** dialog box, configure the start time and end time that you want the rule to be active or not active.

6 In the **Month** drop-down list, select either **All** or a specific month.

7 Check the box for the time frame that you want.

If you check **Specify days**, check one or more of the listed days.

8 Click **OK**.

9 In the **Schedule** list, do one of the following actions:

To keep the rule active during this time	Uncheck the box in the **Any Time Except** column.
To make the rule inactive during this time	Check the box in the **Any Time Except** column.

10 Click **OK**.

See "Setting up firewall rules" on page 446.

See "Customizing firewall rules" on page 450.

See "Editing a policy" on page 297.

Managing intrusion prevention

This chapter includes the following topics:

- Managing intrusion prevention on your client computers

- How intrusion prevention works

- About Symantec IPS signatures

- About custom IPS signatures

- Enabling or disabling network intrusion prevention or browser intrusion prevention

- Creating exceptions for IPS signatures

- Setting up a list of excluded computers

- Configuring client intrusion prevention notifications

- Managing custom intrusion prevention signatures

Managing intrusion prevention on your client computers

The default intrusion prevention settings protect client computers against a wide variety of threats. You can change the default settings for your network.

| Table 21-1 | Managing intrusion prevention |

Task	Description
Learn about intrusion prevention	Learn how intrusion prevention detects and blocks network and browser attacks.
	See "How intrusion prevention works" on page 464.
	See "About Symantec IPS signatures" on page 465.
Enable or disable intrusion prevention	You might want to disable intrusion prevention for troubleshooting purposes or if client computers detect excessive false positives. However, to keep your client computers secure, typically you should not disable intrusion prevention.
	You can enable or disable the following types of intrusion prevention in the Intrusion Prevention policy:
	■ Network intrusion prevention ■ Browser intrusion prevention
	See "Enabling or disabling network intrusion prevention or browser intrusion prevention" on page 467.
	You can also enable or disable both types of intrusion prevention, as well as the firewall, when you run the **Enable Network Threat Protection** or **Disable Network Threat Protection** command.
	See "Running commands on the client computer from the console" on page 233.

Table 21-1	Managing intrusion prevention *(continued)*
Task	**Description**
Create exceptions to change the default behavior of Symantec network intrusion prevention signatures	You might want to create exceptions to change the default behavior of the default Symantec network intrusion prevention signatures. Some signatures block the traffic by default and other signatures allow the traffic by default.
	Note: You cannot change the behavior of browser intrusion prevention signatures.
	You might want to change the default behavior of some network signatures for the following reasons:
	■ Reduce consumption on your client computers. For example, you might want to reduce the number of signatures that block traffic. Make sure, however, that an attack signature poses no threat before you exclude it from blocking.
	■ Allow some network signatures that Symantec blocks by default. For example, you might want to create exceptions to reduce false positives when benign network activity matches an attack signature. If you know the network activity is safe, you can create an exception.
	■ Block some signatures that Symantec allows. For example, Symantec includes signatures for peer-to-peer applications and allows the traffic by default. You can create exceptions to block the traffic instead.
	See "Creating exceptions for IPS signatures" on page 467.
	You can use application control to prevent users from running peer-to-peer applications on their computers.
	See "Typical application control rules" on page 489.
	If you want to block the ports that send and receive peer-to-peer traffic, use a Firewall policy.
	See "Creating a firewall policy" on page 416.
Create exceptions to ignore browser signatures on client computers	You can create exceptions to exclude browser signatures from browser intrusion prevention.
	You might want to ignore browser signatures if browser intrusion prevention causes problems with browsers in your network.
	See "Creating exceptions for IPS signatures" on page 467.

<div align="center">

Table 21-1   Managing intrusion prevention *(continued)*

</div>

Task	Description
Exclude specific computers from intrusion prevention scans	You might want to exclude certain computers from intrusion prevention. For example, some computers in your internal network may be set up for testing purposes. You might want Symantec Endpoint Protection to ignore the traffic that goes to and from those computers.
	When you exclude computers, you also exclude them from the denial of service protection and port scan protection that the firewall provides.
	See "Setting up a list of excluded computers" on page 469.
Configure intrusion prevention notifications	By default, messages appear on client computers for intrusion attempts. You can customize the message.
	See "Configuring client intrusion prevention notifications" on page 470.
Create custom intrusion prevention signatures	You can write your own intrusion prevention signature to identify a specific threat. When you write your own signature, you can reduce the possibility that the signature causes a false positive.
	For example, you might want to use custom intrusion prevention signatures to block and log Web sites.
	See "Managing custom intrusion prevention signatures" on page 471.
Monitor intrusion prevention	Regularly check that intrusion prevention is enabled on the client computers in your network.
	See "Monitoring endpoint protection" on page 603.

How intrusion prevention works

Intrusion prevention is part of Network Threat Protection.

Intrusion prevention automatically detects and blocks network attacks and attacks on browsers. Intrusion prevention is the second layer of defense after the firewall to protect client computers. Intrusion prevention is sometimes called the intrusion prevention system (IPS).

Intrusion prevention intercepts data at the network layer. It uses signatures to scan packets or streams of packets. It scans each packet individually by looking for the patterns that correspond to network attacks or browser attacks. Intrusion prevention detects attacks on operating system components and the application layer.

Intrusion prevention provides two types of protection.

Table 21-2   Types of intrusion prevention

Type	Description
Network intrusion prevention	Network intrusion prevention uses signatures to identify attacks on client computers. For known attacks, intrusion prevention automatically discards the packets that match the signatures.
	You can also create your own custom network signatures as part of an Intrusion Prevention policy. You cannot create custom signatures on the client directly; however, you can import custom signatures on the client.
	See "About Symantec IPS signatures" on page 465.
Browser intrusion prevention	Browser intrusion prevention monitors attacks on Internet Explorer and Firefox. Browser intrusion prevention is not supported on any other browsers.
	Firefox might disable the Symantec Endpoint Protection plug-in, but you can re-enable it.
	This type of intrusion prevention uses attack signatures as well as heuristics to identify attacks on browsers.
	For some browser attacks, intrusion prevention requires that the client terminate the browser. A notification appears on the client computer.
	See the following knowledge base article for the latest information about the browsers that browser intrusion prevention protects: Supported browser versions for browser intrusion prevention.

See "Managing intrusion prevention on your client computers" on page 461.

About Symantec IPS signatures

Symantec intrusion prevention signatures are installed on the client by default.

See "Managing intrusion prevention on your client computers" on page 461.

Intrusion prevention uses the Symantec signatures to monitor individual packets or streams of packets. For streams of packets, intrusion prevention can remember the list of patterns or partial patterns from previous packets. It can then apply this information to subsequent packet inspections.

Symantec signatures include signatures for network intrusion prevention and browser intrusion prevention.

Network intrusion prevention signatures	Network signatures match patterns of an attack that can crash applications or exploit the operating systems on your client computers.
	You can change whether a Symantec network signature blocks or allows traffic. You can also change whether or not Symantec Endpoint Protection logs a detection from a signature in the Security log.
Browser intrusion prevention signatures	Browser signatures match patterns of attack on supported browsers, such as script files that can crash the browser.
	You cannot customize the action or log setting for browser signatures, but you can exclude a browser signature.

See "Creating exceptions for IPS signatures" on page 467.

The Symantec Security Response team supplies the attack signatures. The intrusion prevention engine and the corresponding set of signatures are installed on the client by default. The signatures are part of the content that you update on the client.

You can view information about IPS signatures on the following Symantec Web site page:

Attack Signatures

About custom IPS signatures

You can create your own IPS network signatures. These signatures are packet-based.

Unlike Symantec signatures, custom signatures scan single packet payloads only. However, custom signatures can detect attacks in the TCP/IP stack earlier than the Symantec signatures.

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.

You can specify whether or not Symantec Endpoint Protection logs a detection from custom signatures in the Packet log.

See "Managing custom intrusion prevention signatures" on page 471.

Enabling or disabling network intrusion prevention or browser intrusion prevention

You can enable or disable either type of intrusion prevention. Typically, you should not disable either type of intrusion prevention.

See "Managing intrusion prevention on your client computers" on page 461.

You can also exclude particular computers from network intrusion prevention.

See "Setting up a list of excluded computers" on page 469.

Note: To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

See "Configuring firewall settings for mixed control" on page 421.

Enabling or disabling network intrusion prevention or browser intrusion prevention

1   In the console, open an Intrusion Prevention policy.

2   On the **Intrusion Prevention Policy** page, click **Settings**.

3   Check or uncheck the following options:

   - **Enable Network Intrusion Prevention**

   - **Enable Browser Intrusion Prevention**

4   Click the icon to lock or unlock the options on client computers. When you lock an option, you prevent user changes to the option.

5   Click **OK**.

Creating exceptions for IPS signatures

You can create exceptions to perform the following actions:

- Change the default behavior of IPS network signatures.

- Specify the browser signatures that client computers should ignore.

You can change the action that the client takes when the IPS recognizes a network signature. You can also change whether the client logs the event in the Security log.

You cannot change the behavior of Symantec browser signatures; unlike network signatures, browser signatures do not allow custom action and logging settings. However, you can create an exception for a browser signature so that clients ignore the signature.

Note: When you add a browser signature exception, Symantec Endpoint Protection Manager includes the signature in the exceptions list and automatically sets the action to **Allow** and the log setting to **Do Not Block**. You cannot customize the action or the log setting.

See

Note: To change the behavior of a custom IPS signature that you create or import, you edit the signature directly.

To change the behavior of Symantec IPS network signatures

1   In the console, open an Intrusion Prevention policy.

2   On the **Intrusion Prevention Policy** page, click **Exceptions**, and then click **Add**.

3   In the **Add Intrusion Prevention Exceptions** dialog box, do one of the following actions to filter the signatures:

   ■   To display the signatures in a particular category, select an option from the **Show category** drop-down list.

   ■   To display the signatures that are classified with a particular severity, select an option from the **Show severity** drop-down list.

4   Select one or more signatures.

   To make the behavior for all network signatures the same, click **Select All**.

5   Click **Next**.

6   In the **Signature Action** dialog box, set the action to **Block** or **Allow**.

   Note: The **Signature Action** dialog only applies to network signatures.

7   Optionally, set the log action to **Log the traffic** or **Do not log the traffic**.

8   Click **OK**.

   If you want to revert the network signature's behavior back to the original behavior, select the signature and click **Delete**.

   If you want clients to use the browser signature and not ignore it, select the signature and click **Delete**.

9   Click **OK**.

Setting up a list of excluded computers

You can set up a list of computers for which the client does not match attack signatures or check for port scans or denial-of-service attacks. The client allows all inbound traffic and outbound traffic from these hosts, regardless of the firewall rules and settings or IPS signatures.

You might want to set up a list of computers to exclude from intrusion prevention. Computers might run some legitimate software that intrusion prevention detects as a threat. For example, you might run a vulnerability scanner in your network. Intrusion prevention blocks the vulnerability scanner when it runs. You can exclude the IP address of the vulnerability scanner from intrusion prevention detection.

You might also exclude computers to allow an Internet service provider to scan the ports in your network to ensure compliance with their service agreements. Or, you might have some computers in your internal network that you want to set up for testing purposes.

Note: You can also set up a list of computers that allows all inbound traffic and outbound traffic unless an IPS signature detects an attack. In this case, you create a firewall rule that allows all hosts.

To set up a list of excluded computers

1   In the console, open an Intrusion Prevention policy.

2   On the **Intrusion Prevention Policy** page, click **Settings**.

3   If not checked already, check **Enable excluded hosts** and then click **Excluded Hosts**.

4   In the **Excluded Hosts** dialog box, check **Enabled** next to any host group that you want to exclude.

    See

5   To add the hosts that you want to exclude, click **Add**.

6   In the **Host** dialog box, in the drop-down list, select one of the following host types:

    ■ IP address

    ■ IP range

    ■ Subnet

7   Enter the appropriate information that is associated with the host type you selected.

For more information about these options, click **Help**.

8   Click **OK**.

9   Repeat 5 and 8 to add additional devices and computers to the list of excluded computers.

10   To edit or delete any of the excluded hosts, select a row, and then click **Edit** or **Delete**.

11   Click **OK**.

12   When you finish configuring the policy, click **OK**.

Configuring client intrusion prevention notifications

By default, notifications appear on client computers when the client detects intrusion protection events. When these notifications are enabled, they display a standard message. You can add customized text to the standard message.

To client configure intrusion prevention notifications

1   In the console, click **Clients** and under **Clients**, select a group.

2   On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.

3   To the right of **Client User Interface Control Settings**, click **Tasks** , and then click **Edit Settings**.

4   In the **Client User Interface Control Settings for *group name*** dialog box, click either **Server control** or **Mixed control**.

5   Beside **Mixed control** or **Server control**, click **Customize**.

If you click **Mixed control**, on the **Client/Server Control Settings tab**, beside **Show/Hide Intrusion Prevention notifications**, click **Server**. Then click the **Client User Interface Settings** tab.

6   In the **Client User Interface Settings** dialog box or tab, click **Display Intrusion Prevention notifications**.

7   To enable a beep when the notification appears, click **Use sound when notifying users**.

8   Click **OK**.

9   Click **OK**.

See "Managing intrusion prevention on your client computers" on page 461.

Managing custom intrusion prevention signatures

You can write your own network intrusion prevention 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.

Warning: You should be familiar with the TCP, UDP, or ICMP protocols before you develop intrusion prevention signatures. An incorrectly formed signature can corrupt the custom signature library and damage the integrity of the clients.

Table 21-3 Managing custom intrusion prevention signatures

Task	Description
Create a custom library with a signature group	You must create a custom library to contain your custom signatures. When you create a custom library, you use signature groups to manage the signatures more easily. You must add at least one signature group to a custom signature library before you add the signatures. See "Creating a custom IPS library" on page 472.
Add custom IPS signatures to a custom library	You add custom IPS signatures to a signature group in a custom library. See "Adding signatures to a custom IPS library" on page 472.
Assign libraries to client groups	You assign custom libraries to client groups rather than to a location. See "Assigning multiple custom IPS libraries to a group" on page 474.
Change the order of signatures	Intrusion prevention uses the first rule match. Symantec Endpoint Protection checks the signatures in the order that they are listed in the signatures list. For example, if you add a signature group to block TCP traffic in both directions on destination port 80, you might add the following signatures: ■ Block all traffic on port 80. ■ Allow all traffic on port 80. If the Block all traffic signature is listed first, the Allow all traffic signature is never enacted. If the Allow all traffic signature is listed first, the Block all traffic signature is never enacted, and all HTTP traffic is always allowed. **Note:** Firewall rules take precedence over intrusion prevention signatures. See "Changing the order of custom IPS signatures" on page 475.
Copy and paste signatures	You can copy and paste signatures between groups and between libraries. See "Copying and pasting custom IPS signatures" on page 475.

Task	Description
Define variables for signatures	When you add a custom signature, you can use variables to represent changeable data in signatures. If the data changes, you can edit the variable instead of editing the signatures throughout the library.
	See "Defining variables for custom IPS signatures" on page 476.
Test custom signatures	You should test the custom intrusion prevention signatures to make sure that they work.
	See "Testing custom IPS signatures" on page 477.

Creating a custom IPS library

You create a custom IPS library to contain your custom IPS signatures.

See "Managing custom intrusion prevention signatures" on page 471.

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.

   See "Adding signatures to a custom IPS library" on page 472.

Adding signatures to a custom IPS library

You add custom intrusion prevention signatures to a new or existing custom IPS library.

See "Managing custom intrusion prevention signatures" on page 471.

To add a custom signature

1   Create a custom IPS library.

    See "Creating a custom IPS library" on page 472.

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, signatures for some common protocols use the following syntax:

    HTTP   rule tcp, dest=(80,443), saddr=$LOCALHOST,
                    msg="MP3 GET in HTTP detected",
                    regexpcontent="[Gg][Ee][Tt] .*[Mm][Pp]3 .*"

    FTP   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"

    For more information about the syntax, click **Help**.

7   If you want an application to trigger the signature, click **Add**.

8   In the **Add Application** dialog box, type the file name and an optional
    description for the application.

    For example, to add the application Internet Explorer, type the file name as
    iexplore or **iexplore.exe**. If you do not specify a file name, any application
    can trigger the signature.

9   Click **OK**.

    The added application is enabled by default. If you want to disable the
    application until a later time, uncheck the check box in the **Enabled** column.

10 In the **Action** group box, select the action you want the client to take when the signature detects the event:

Block   Identifies and blocks the event or attack and records it in the Security Log

Allow   Identifies and allows the event or attack and records it in the Security Log

11 To record the event or attack in the Packet Log, check **Write to Packet Log**.

12 Click **OK**.

The added signature is enabled by default. If you want to disable the signature until a later time, uncheck the check box in the **Enabled** column.

13 You can add additional signatures. When you are finished, click **OK**.

14 If you are prompted, assign the custom IPS signatures to a group.

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

See "Assigning multiple custom IPS libraries to a group" on page 474.

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.

See "Managing custom intrusion prevention signatures" on page 471.

To assign multiple custom IPS libraries to a group

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

2 Under **Clients**, select the group to which you want to assign the custom signatures.

3 On the **Policies** tab, under **Location-independent Policies and Settings**, click **Custom Intrusion Prevention**.

4 In the **Custom Intrusion Prevention for** *group name* dialog box, check the check box in the **Enabled** column for each custom IPS library you want to assign to that group.

5 Click **OK**.

Changing the order of custom IPS signatures

The IPS engine for custom signatures checks the signatures in the order that they are listed in the signatures list. Only one signature is triggered per packet. When a signature matches an inbound traffic packet or outbound traffic packet, the IPS engine stops checking other signatures. So that the IPS engine executes signatures in the correct order, you can change the order of the signatures in the signatures list. If multiple signatures match, move the higher priority signatures to the top.

For example, if you add a signature group to block TCP traffic in both directions on destination port 80, you might add the following signatures:

■ Block all traffic on port 80.

■ Allow all traffic on port 80.

If the Block all traffic signature is listed first, the Allow all traffic signature is never enacted. If the Allow all traffic signature is listed first, the Block all traffic signature is never enacted, and all HTTP traffic is always allowed.

Note: Firewall rules take precedence over intrusion prevention signatures.

See "Managing custom intrusion prevention signatures" on page 471.

To change the order of custom IPS signatures

1   Open a custom IPS library.

2   On the **Signatures** tab, in the **Signatures for this Group** table, select the signature that you want to move, and then do one of the following actions:

■ To process this signature before the signature above it, click **Move Up**.

■ To process this signature after the signature below it, click **Move Down**.

3   When you finish configuring this library, click **OK**.

Copying and pasting custom IPS signatures

You can copy and paste signatures within the same signature group, between signature groups, or between signature libraries. For example, you may realize that you added a signature to the wrong signature group. Or you may want to have two signatures that are nearly identical.

See "Managing custom intrusion prevention signatures" on page 471.

To copy and paste custom IPS signatures

1   Open a custom IPS library.

2   In the **Custom Intrusion Prevention Signature**s dialog box, in the **Signatures** tab, in the **Signatures for this Group** table, right-click the signature you want to copy, and then click **Copy**.

3   Right-click the signatures list, and then click **Paste**.

4   When you finish configuring this library, click **OK**.

Defining variables for custom IPS signatures

When you add a custom IPS signature, you can use variables to represent changeable data in signatures. If the data changes, you can edit the variable instead of editing the signatures throughout the library.

See "Managing custom intrusion prevention signatures" on page 471.

Before you can use the variables in the signature, you must define them. The variables that you define in the custom signature library can then be used in any signature in that library.

You can copy and paste the content from the existing sample variable to start as a basis for creating content.

To define variables for custom IPS signatures

1   Create a custom IPS library.

2   In the **Custom Intrusion Prevention Signatures** dialog box, click the **Variables** tab.

3   Click **Add**.

4   In the **Add Variable** dialog box, type a name and optional description for the variable.

5   Add a content string for the variable value of up to 255 characters.

    When you enter the variable content string, follow the same syntax guidelines that you use for entering values into signature content.

6   Click **OK**.

    After the variable is added to the table, you can use the variable in any signature in the custom library.

To use variables in custom IPS signatures

1   On the **Signatures** tab, add or edit a signature.

2   In the **Add Signature** or **Edit Signature** dialog box, in the **Content** field, type the variable name with a dollar sign ($) in front of it.

    For example, if you create a variable named HTTP for specifying HTTP ports, type the following:

    $HTTP

3   Click **OK**.

4   When you finish configuring this library, click **OK**.

Testing custom IPS signatures

After you create custom IPS signatures, you should test them to make sure that they function correctly.

Table 21-4   Testing custom IPS signatures

Step	Action	Description
Step 1	Make sure that clients use the current Intrusion Prevention policy	The next time that the client receives the policy, the client applies the new custom signatures.
		See "How the client computers get policy updates" on page 307.
Step 2	Test the signature content on the client	You should test the traffic that you want to block on the client computers.
		For example, if your custom IPS signatures should block MP3 files, try to download some MP3 files to the client computers. If the download does not occur, or times out after many tries, the custom IPS signature is successful.
		You can click Help for more information about the syntax that you can use in custom IPS signatures.
Step 3	View blocked events in Symantec Endpoint Protection Manager	You can view events in the Network Threat Protection Attack logs. The message you specify in the custom IPS signature appears in the log.
		See "Monitoring endpoint protection" on page 603.

See "Managing custom intrusion prevention signatures" on page 471.

Managing application and device control

This chapter includes the following topics:

- About application and device control
- About Application and Device Control policies
- About the structure of an Application and Device Control policy
- Setting up application and device control
- Enabling a default application control rule set
- Creating custom application control rules
- Configuring system lockdown
- Managing device control

About application and device control

You can use application and device control to monitor and control the behavior of applications on client computers and manage hardware devices that access client computers. You can also control applications by setting up system lockdown to allow only approved applications on client computers.

Note: Both application control and device control are supported on 32-bit and 64-bit computers.

You use an Application and Device Control policy to configure application control and device control on client computers. You use the **Policies** tab on the **Clients** page to set up system lockdown.

Warning: Application control and system lockdown are advanced security features that only experienced administrators should configure.

A summary of the application and device control features is given here.

Application control	You can use application control to control applications in the following ways:
	■ Prevent malware from taking over applications
	■ Restrict the applications that can run
	■ Prevent users from changing configuration files
	■ Protect specific registry keys
	■ Protect particular folders, such as \WINDOWS\system
Device control	You can use device control to control devices in the following ways:
	■ Block or allow different types of devices that attach to client computers, such as USB, infrared, and FireWire devices
	■ Block or allow serial ports and parallel ports
System lockdown	You can use system lockdown to control applications in the following ways:
	■ Control the applications on your client computers.
	■ Block almost any Trojan horse, spyware, or malware that tries to run or load itself into an existing application.
	System lockdown ensures that your system stays in a known and trusted state.
	Note: If you do not implement system lockdown carefully, it can cause serious problems in your network. Symantec recommends that you implement system lockdown in specific stages.
	See "Configuring system lockdown" on page 497.

See "About Application and Device Control policies" on page 481.

See "Setting up application and device control" on page 482.

About Application and Device Control policies

You can implement access control or device control on client computers by using an Application and Device Control policy. You can only assign one Application and Device Control policy at a time to a group or a location.

See "About application and device control" on page 479.

By default, there is an Application and Device Control policy on the management server. However, by default the Application and Device Control policy driver is disabled on the client. To enable the driver, you must either enable an existing rule or add and enable a new rule in the policy. After the policy is applied to the client computer, a notification requests that the user restart the client computer. The user must restart the computer for the policy to take effect.

If you withdraw or disable the Application and Device Control policy, the driver is disabled and the client is not protected. When you re-enable the policy, the user must restart the client computer again.

About the structure of an Application and Device Control policy

The application control portion of an Application and Device Control policy can contain multiple rule sets, and each rule set contains one or more rules. You can configure properties for a rule set, and properties, conditions, and actions for each rule.

Rules control attempts to access computer entities, such as files or Windows registry keys, that Symantec Endpoint Protection monitors. You configure these different types of attempts as conditions. For each condition, you can configure actions to take when the condition is met. You configure rules to apply to only certain applications, and you can optionally configure them to exclude other applications from having the action applied.

See "Creating custom application control rules" on page 485.

Device control consists of a list of blocked devices and a list of devices that are excluded from blocking. You can add to these two lists and manage their contents.

Figure 22-1 illustrates the application and device control components and how they relate to each other.

Figure 22-1   Application and Device Control policy structure
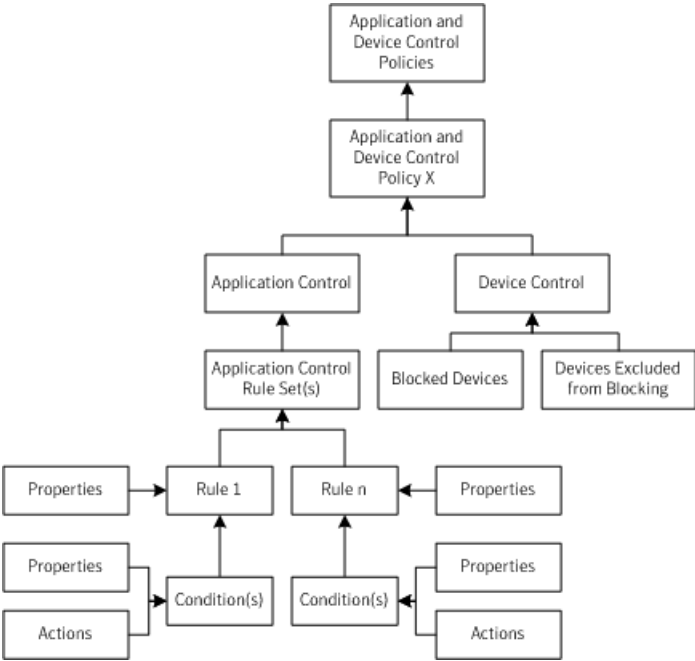
Setting up application and device control

You can set up application and device control by performing some typical tasks.

See "About application and device control" on page 479.

Task	Description
Enable default application control rule sets	Application and Device Control policies contain default application control rule sets. The default rule sets are disabled. You can enable any sets that you need. **Note:** If the default rule sets do not meet your requirements, create custom rule sets. The default rule sets are configured in production mode rather than test mode. However, you can change the setting to test mode and test the rules in your test network before you apply them to your production network. See "Enabling a default application control rule set" on page 484. **Note:** Client computers require a restart when you enable application control rules. See "Restarting client computers" on page 145.
Create and test custom application control rule sets	You can create custom application control rule sets. Typically only advanced administrators should perform this task. See "Creating custom application control rules" on page 485. See "Typical application control rules" on page 489. **Note:** Client computers require a restart when you enable application control rules.
Create exceptions for application control	Application control might cause problems for some applications that you run in your network. You can exclude files or folders from application control. You use an Exceptions policy to specify the exception. **Note:** Symantec Endpoint Protection 12.1 included a separate application control exception. In the current release, an application control exception is created as part of the file or folder exceptions configuration. See "Excluding a file or a folder from scans" on page 534.
Set up system lockdown	System lockdown controls the applications on your client computers. See "Configuring system lockdown" on page 497.
Configure device control to allow or block hardware devices	Device control specifies what hardware devices are allowed or blocked on your client computers. Symantec Endpoint Protection Manager provides a device list that you can use in the device control configuration. You can add devices to the list. See "Managing device control" on page 521.

Table 22-1   Setting up application and device control

<div style="text-align:center">**Table 22-1**   Setting up application and device control *(continued)*</div>

Task	Description
View the Application Control and Device Control logs	You can view the application control and device control events in the Application Control log and the Device Control log in Symantec Endpoint Protection Manager.
	On the client computer, application control and device control events appear in the Control log.
	Note: You might see duplicate or multiple log entries for a single application control action. For example, if explorer.exe tries to copy a file, it sets the write and delete bits of the file's access mask. Symantec Endpoint Protection logs the event. If the copy action fails because an application control rule blocks the action, explorer.exe tries to copy the file by using only the delete bit in the access mask. Symantec Endpoint Protection logs another event for the copy attempt.
Prevent or allow users from enabling or disabling application and device control	You can prevent or allow users from enabling or disabling application and device control on the client. Use the setting in the **Client User Interface Settings** dialog.
	See "Changing the user control level" on page 239.

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.

If you want to use the default rule sets in an Application and Device Control policy, you must enable them.

See "Setting up application and device control" on page 482.

To enable a default application control rule set

1   In the console, in the Application and Device Control policy to which you want to add a default application control rule set, click **Application Control**.

2   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.

3   When you have finished reviewing the rules and their condition settings, click **Cancel**.

4   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.

5   Click **OK**.

To test the rule set Block writing to USB drives

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 custom application control rules

You might want to use custom application control rules when you set up application and device control.

See "Setting up application and device control" on page 482.

Table 22-2   Creating custom application control rules

Step	Action	Description
Step 1	Plan the rule set	A new application rule set contains one or more administrator-defined rules. Each rule set and each rule has properties. Each rule can contain one or more conditions for monitoring applications and their access to specified files, folders, registry keys, and processes.
		You should review best practices before you create custom rules.
		See "About best practices for creating application control rules" on page 487.
		You can also review the structure of the default rule sets to see how they are constructed.

Table 22-2   Creating custom application control rules *(continued)*

Step	Action	Description
Step 2	Create the rule set and add rules	You can create multiple rules and add them to a single application control rule set. 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. See "Creating a custom rule set and adding rules" on page 491. See "Typical application control rules" on page 489. You can copy and paste rule sets or individual rules within the same policy or between two policies. You might want to copy rules from the policies that you download from Symantec or from the test policies that contain rules that you want to use in production policies. See "Copying application rule sets or rules between Application and Device Control policies" on page 492.
Step 3	Apply a rule to specific applications and exclude certain applications from the rule	Every rule must have at least one application to which it applies. You can also exclude certain applications from the rule. You specify the applications on the **Properties** tab for the rule. See "Applying a rule to specific applications and excluding applications from a rule" on page 493.

Table 22-2   Creating custom application control rules *(continued)*

Step	Action	Description
Step 4	Add conditions and actions to rules	The condition specifies what the application tries to do when you want to control it. You can set any of the following conditions: ■ Registry access attempts ■ File and folder access attempts ■ Launch process attempts ■ Terminate process attempts ■ Load DLL attempts See "Adding conditions and actions to a custom application control rule" on page 495. You can configure any of the following actions to take on an application when it meets the configured condition: ■ Continue processing other rules. ■ Allow the application to access the entity. ■ Block the application from accessing the entity. ■ Terminate the application that tries to access an entity. **Note:** Remember that actions always apply to the process that is defined for the rule. They do not apply to a process that you define in a condition.
Step 5	Test the rules	You should test your rules before you apply them to your production network. Configuration errors in the rule sets that are used in an Application and Device Control policy can disable a computer or a server. The client computer can fail, or its communication with Symantec Endpoint Protection Manager can be blocked. See "Testing application control rule sets" on page 496. After you test the rules, you can apply them to your production network.

About best practices for creating application control rules

You should plan your custom application control rules carefully.

See "Creating custom application control rules" on page 485.

See "Typical application control rules" on page 489.

When you create application control rules, keep in mind the following best practices:

Table 22-3   Best practices for application control rules

Best practice	Description	Example
Use one rule set per goal	A best practice is to create one rule set that includes all of the actions that allow, block, and monitor one given task.	You want to block write attempts to all removable drives and you want to block applications from tampering with a particular application. To accomplish these goals, you should create two different rule sets. You should not create all of the necessary rules to accomplish both of these goals with one rule set.
Consider the rule order	Application control rules work similarly to most network-based firewall rules in that both use the first rule match feature. When multiple conditions are true, the first rule is the only one that is applied unless the action that is configured for the rule is to **Continue processing other rules**.	You want to prevent all users from moving, copying, and creating files on USB drives. You have an existing rule with a condition that allows write access to a file named Test.doc. You add 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. The **Allow access** to Test.doc condition comes before the **Block access** to USB drives condition in the rule set. The **Block access** to USB drives condition does not get processed when the condition that precedes it in the list is true.

Table 22-3   Best practices for application control rules *(continued)*

Best practice	Description	Example
Use the Terminate process action sparingly	The **Terminate process** action kills a process when the process meets the configured condition. Only advanced administrators should use the **Terminate process** action. Typically, you should use the **Block access** action instead.	You want to terminate Winword.exe any time that any process launches Winword.exe. You create a rule and configure it with the **Launch Process Attempts** condition and the **Terminate process** action. You apply the condition to Winword.exe and apply the rule to all processes. You might expect this rule to terminate Winword.exe, but that is not what the rule does. If you try to start Winword.exe from Windows Explorer, a rule with this configuration terminates Explorer.exe, not Winword.exe. Users can still run Winword.exe if they launch it directly.
Use the Terminate Process Attempts condition to protect processes	The **Terminate Process Attempts** condition allows or blocks an application's ability to terminate a process on a client computer. The condition does not allow or prevent users from stopping an application by the usual methods, such as clicking Quit from the File menu.	Process Explorer is a tool that displays the DLL processes that have opened or loaded, and what resources the processes use. You might want to terminate Process Explorer when it tries to terminate a particular application. Use the **Terminate Process Attempts** condition and the **Terminate process** action to create this type of rule. You apply the condition to the Process Explorer application. You apply the rule to the application or applications that you do not want Process Explorer to terminate.

Typical application control rules

You might want to create custom application control rules to prevent users from opening applications, writing to files, or sharing files.

See "Creating custom application control rules" on page 485.

You can look at the default rule sets to help determine how to set up your rules. For example, you can edit the **Block applications from running** rule set to view how you might use a **Launch Process Attempts** condition.

See "Enabling a default application control rule set" on page 484.

Table 22-4	Typical application control rules

Rule	Description
Prevent users from opening an application	You can block an application when it meets either of these conditions: ■ **Launch Process Attempts** For example, to prevent users from transferring FTP files, you can add a rule that blocks a user from launching an FTP client from the command prompt. ■ **Load DLL Attempts** For example, if you add a rule that blocks Msvcrt.dll on the client computer, users cannot open Microsoft WordPad. The rule also blocks any other application that uses the DLL.
Prevent users from writing to a particular file	You may want to let users open a file but not modify the file. For example, a file may include the financial data that employees should view but not edit. You can create a rule to give users read-only access to a file. For example, you can add a rule that lets you open a text file in Notepad but does not let you edit it. Use the **File and Folder Access Attempts** condition to create this type of rule.
Block file shares on Windows computers	You can create a custom rule that applies to all applications to disable local file and print sharing on Windows computers. Include the following conditions: ■ **Registry Access Attempts** Add all the relevant Windows security and sharing registry keys. ■ **Launch Process Attempts** Specify the server service process (svchost.exe). ■ **Load DLL Attempts** Specify the DLLs for the Security and Sharing tabs (rshx32.dll, ntshrui.dll). ■ **Load DLL Attempts** Specify the server service DLL (srvsvc.dll). You set the action for each condition to **Block access**. **Note:** After you apply the policy, you must restart client computers to completely disable file sharing. You can also use firewall rules to prevent or allow client computers to share files. See "Permitting clients to browse for files and printers in the network" on page 455.

Table 22-4   Typical application control rules *(continued)*

Rule	Description
Prevent users from running peer-to-peer applications	You can use application control to prevent users from running peer-to-peer applications on their computers.
	You can create a custom rule with a **Launch Process Attempts** condition. In the condition, you must specify all peer-to-peer applications that you want to block, such as LimeWire.exe or *.torrent. You can set the action for the condition to **Block access** or **Terminate process**.
	Use an Intrusion Prevention policy to block network traffic from peer-to-peer applications. Use a Firewall policy to block the ports that send and receive peer-to-peer application traffic.
	See "Managing intrusion prevention on your client computers" on page 461.
	See "Creating a firewall policy" on page 416.
Block write attempts to DVD drives	Currently, Symantec Endpoint Protection Manager does not support a rule set that specifies the blocking of write attempts to DVD drives. You can select the option in the Application and Device Control policy, however, the option is not enforced. Instead, you can create an Application and Device Control policy that blocks specific applications that write to DVD drives.
	You should also create a Host Integrity policy that sets the Windows registry key to block write attempts to DVD drives.

Creating a custom rule set and adding rules

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.

Note: If you create a custom rule that blocks access to a 32-bit-specific folder (such as Windows\system32), the rules does not work on 64-bit clients. You must also create a rule to block access to the Windows\syswow64 folder as well.

See "Creating custom application control rules" on page 485.

Creating a custom rule set and adding rules

1. In the console, open an Application and Device Control policy and click **Add**.

2. In the **Add Application Control Rule Set** dialog box, uncheck **Enable logging** if you do not want to log events about this rule set.

3   In the **Rule set name** text box, change the default name for the rule set.

4   In the **Description** field, type a description.

5   Change the default name for the rule in the **Rule name** text box, and then type a description of the rule

6   Uncheck **Enable this rule** if you do not want to enable the rule at this time.

7   On the **Properties** tab, you specify the applications to which this rule applies and what applications should be excluded from the rule.

Each rule must have an application to which it applies.

See "Applying a rule to specific applications and excluding applications from a rule" on page 493.

Each rule must also have conditions and actions.

See "Adding conditions and actions to a custom application control rule" on page 495.

8   To add additional rules to the rule set, click **Add**, and then click **Add Rule**.

9   Click **OK**.

The new rule set appears and is configured for test mode. You should test new rule sets before you apply them to your client computers.

See "Testing application control rule sets" on page 496.

Copying application rule sets or rules between Application and Device Control policies

You can copy application control rule sets or individual rules between two different policies. You can also copy rule sets or rules within the same policy. The procedures here describe how to copy rule sets or rules between two different policies.

See "Creating custom application control rules" on page 485.

Copying application rule sets between Application and Device Control policies

1   In the console, open the Application and Device Control policy that contains the rule sets that you want to copy.

2   Click **Application Control**.

3   On the **Application Control** page, under **Application Control Rules Sets**, right-click the rule set that you want to copy, and then select **Copy**.

4   Click **OK** to close the current policy.

5 In the console, under **Application and Device Control Policies**, select the target policy.

Under **Tasks**, click **Edit the policy**.

6 In the target policy, select **Application Control**.

7 Under **Application Control Rule Sets**, right-click and select **Paste**.

Copying application rules between Application and Device Control policies

1 In the console, open the Application and Device Control policy that contains the rule that you want to copy.

2 Click **Application Control**.

3 Select the rule set that you want to copy the rule from, and then click **Edit**.

4 Under **Rules**, right-click the rule that you want to copy and select **Copy**.

5 Click **OK** to close the rule set.

6 Click **OK** to close the policy.

7 In the console, under **Application and Device Control Policies**, select the target policy.

8 Under **Tasks**, click **Edit the policy**.

9 In the target policy, select **Application Control**.

10 Select the rule set to which you want to copy the rule, and then click **Edit**.

11 Under **Rules**, right-click and select **Paste**.

Applying a rule to specific applications and excluding applications from a rule

You can apply a rule to applications, and you can exclude applications from the rule's actions. You specify one list that contains the applications to which the rule applies (the inclusions). You specify another list that contains the applications to which the rule does not apply (the exclusions). To tie a rule to a specific application, you define that application in the Apply this rule to the following processes text field.

If you want to tie the rule to all applications except for a given set of applications, then you can use the following settings:

■ In the Apply this rule to the following processes text box, define a wildcard character for all processes (*).

■ In the Do not apply this rule to the following processes text box, list the applications that need an exception.

You can define as many applications as you want for each list.

Note: Every rule must have at least one application listed in the **Apply this rule to the following processes** text box.

When you add applications to a rule, you can use the following ways to specify the application:

- The process name

- Wildcard characters

- Regular expressions

- File fingerprints

- The drive types from where the application was launched

- The device ID

See "Creating custom application control rules" on page 485.

To apply a rule to specific applications and to exclude a rule

1   In the **Edit Application Control Rule Set** dialog box, click the rule that you want to apply.

2   If you want to configure an application to apply the rule to, then to the right of Apply this rule to the following processes, click **Add**.

3   In the **Add Process Definition** dialog box, configure the following items:

- Type the name of the application that you want to match in this rule.

- Click either **Use wildcard matching (* and ? supported)** or **Use regular expression matching** for matching the name.

- If desired, check the specific drive types on which to match the process.

- If desired, check **Only match processes running on the following device id type**, and then type a device ID type in the text field or click **Select** to select a device ID type from the list in the Device Selection dialog box to only match the processes that run on devices of that ID type.

- If desired, click **Options** to match processes based on the file fingerprint and to match only the processes that have a designated argument. You can choose to match the arguments exactly or by using regular expression matching.

4   Click **OK**.

You can repeat steps 2 through 4 to add as many applications as you want.

5   If you want to configure one or more applications to exclude from the rule,
    then to the right of the **Do not apply this rule to the following processes** text
    field, click **Add**.

    Repeat the configuration of the applications to exclude as desired. You have
    the same options when you define an application to exclude as you have when
    you apply the rule to an application.

6   When you have finished defining the applications, click **OK**.

Adding conditions and actions to a custom application control rule

After you define what applications a custom rule applies to, you should define the
conditions and actions for a rule. A condition's properties specify what the
condition looks for. Its actions define what happens when the condition is met.

See "Creating custom application control rules" on page 485.

Adding conditions and actions to an application control rule

1   In the **Add Application Control Rule Set** or **Edit Application Control Rule
    Set** dialog box, under **Rules**, click **Add**, and then click **Add Condition**.

2   Select one of the following conditions:

    ■   **Registry Access Attempts**

    ■   **File and Folder Access Attempts**

    ■   **Launch Process Attempts**

    ■   **Terminate Process Attempts**

    ■   **Load DLL Attempts**

3   On the **Properties** tab for the condition, type a name and a description for
    the condition.

4   To the right of **Apply to the following *entity***, where *entity* represents registry
    keys, files and folders, processes, or DLLs, click **Add**.

5   In the **Add *entity* Definition** dialog box, type the registry key, file or folder
    name, process name, or DLL.

    Note: When you apply a condition to all entities in a particular folder, a best
    practice is to use *folder_name** or *folder_name***. One asterisk includes all
    the files and folders in the named folder. Use *folder_name*** to include every
    file and folder in the named folder plus every file and folder in every subfolder.

    ---

6   Click **OK**.

7 To the right of the **Do not apply to the following processes**, click **Add**, and specify the registry keys, files and folders, processes, or DLLs.

8 Click **OK**.

9 On the **Actions** tab for the condition, select one of the following actions:

- ■ **Continue processing other rules**

- ■ **Allow access**

- ■ **Block access**

- ■ **Terminate process**

For the **Registry Access Attempts** and **File and Folder Access Attempts** conditions, you can configure two sets of actions, one for **Read Attempt** and one for **Create, Delete or Write Attempt**.

10 Check **Enable logging**, and then select a severity level to assign to the entries that are logged.

11 Check **Notify user**, and then type the text that you want to user to see.

12 Click **OK**.

Testing application control rule sets

After you create custom application control rules, you should test them in your network.

See "Creating custom application control rules" on page 485.

Table 22-5   Testing application control rule sets

Step	Description
Configure the rule set for test mode and enable or disable rules	You test rule sets by setting the mode to Test (log only) mode. Test mode creates a log entry to indicate when rules in the rule set would be applied without actually applying the rule.
	Custom rules use Test mode by default. You can also test default rules sets.
	You might want to test rules within the set individually. You can test individual rules by enabling or disabling them in the rule set.
	See "Creating a custom rule set and adding rules" on page 491.
	See "Enabling a default application control rule set" on page 484.
Apply the Application and Device Control policy to computers in your test network	If you created a new Application and Device Control policy, you need to apply the policy to clients in your test network.
	See "Assigning a policy to a group" on page 300.
	Note: Client computers must restart after you apply a new Application and Device Control policy or when you change the default policy.
Check the Control log	After you run your rule sets in Test mode for a period of time, you can check the client's logs for any errors.
	You can view the Application Control log in Symantec Endpoint Protection Manager.
	You can also view the Control log on the client computer.
	When the rules function like you expect them to, you can change the rule set mode to Production mode.

Configuring system lockdown

System lockdown controls applications on a group of client computers by blocking unapproved applications. You can set up system lockdown to allow only applications on a specified list (whitelist). The whitelist comprises all the approved

applications; any other applications are blocked on client computers. Or, you can set up system lockdown to block only applications on a specified list (blacklist). The blacklist comprises all the unapproved applications; any other applications are allowed on client computers.

Note: Any applications that system lockdown allows are subject to other protection features in Symantec Endpoint Protection.

A whitelist or blacklist can include file fingerprint lists and specific application names. A file fingerprint list is a list of file checksums and computer path locations.

You can use an Application and Device Control policy to control specific applications instead of or in addition to system lockdown.

You set up system lockdown for each group or location in your network.

Table 22-6   System lockdown steps

Step	Action	Description
Step 1	Create file fingerprint lists	You can create a file fingerprint list that includes the applications that are allowed or not allowed to run on your client computers. You use the file fingerprint list as part of a whitelist or blacklist in system lockdown.
		Symantec Endpoint Protection provides a checksum utility to create a file fingerprint list. The utility is installed along with Symantec Endpoint Protection on the client computer.
		You can use the utility to create a checksum for a particular application or all the applications in a specified path.
		Note: When you run system lockdown in default or whitelist mode, you need a file fingerprint list that that includes all of the applications you want users to be able to run on their computers. For example, your network might include Windows Vista 32-bit, Windows Vista 64-bit, and Windows XP SP2 clients. You can create a file fingerprint list for each client image that you want to whitelist.
		You can also create a file fingerprint list with any third-party checksum utility.
		See "Creating a file fingerprint list with checksum.exe" on page 505.

<div align="center">**Table 22-6** System lockdown steps *(continued)*</div>

Step	Action	Description
Step 2	Import file fingerprint lists into Symantec Endpoint Protection Manager	After you create the file fingerprint lists, you must import them into Symantec Endpoint Protection Manager. After you import the lists, they are available to add to the system lockdown configuration. See "Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager" on page 506. You can also export existing file fingerprint lists from Symantec Endpoint Protection Manager.
Step 3	Create application name lists for approved or unapproved applications	You can use any text editor to create a text file that includes the file names of the applications that you want to whitelist or blacklist. Unlike file fingerprint lists, you import these files directly into the system lockdown configuration. After you import the files, the applications appear as individual entries in the system lockdown configuration. The import option is only available when blacklist mode is available. You can also manually enter individual application names in the system lockdown configuration. See "Making the blacklist mode for system lockdown appear in Symantec Endpoint Protection Manager" on page 503. **Note:** A large number of named applications might affect client computer performance when system lockdown is enabled in blacklist mode. See "Creating an application name list to import into the system lockdown configuration" on page 508.

Table 22-6   System lockdown steps *(continued)*

Step	Action	Description
Step 4	Set up and test the system lockdown configuration	In test mode, system lockdown is disabled and does not block any applications. All unapproved applications are logged but not blocked. You use the **Log Unapproved Applications Only** option in the **System Lockdown** dialog to test the entire system lockdown configuration.
		To set up and run the test, complete the following steps:
		■ Add file fingerprint lists to the system lockdown configuration. In whitelist mode, the file fingerprints are approved applications. In blacklist mode, the file fingerprints are unapproved applications. ■ Add individual application names or import application name lists into the system lockdown configuration. The import option is only available when blacklist mode is available. You can import a list of application names rather than enter the names one by one in the system lockdown configuration. In whitelist mode, the applications are approved applications. In blacklist mode, the applications are unapproved applications. ■ Run the test for a period of time. Run system lockdown in test mode long enough so that clients run their usual applications. A typical time frame might be one week.
		See "Setting up and testing the system lockdown configuration before you enable system lockdown" on page 514.
Step 5	View the unapproved applications and modify the system lockdown configuration if necessary	After you run the test for a period of time, you can check the list of unapproved applications. You can view the list of unapproved applications by checking the status in the **System Lockdown** dialog box.
		The logged events also appear in the Application Control log.
		You can decide whether to add more applications to the file fingerprint or the applications list. You can also add or remove file fingerprint lists or applications if necessary before you enable system lockdown.
		See "Setting up and testing the system lockdown configuration before you enable system lockdown" on page 514.

Table 22-6   System lockdown steps *(continued)*

Step	Action	Description
Step 6	Enable system lockdown	By default, system lockdown provides only a whitelist mode. You can set up Symantec Endpoint Protection Manager so that system lockdown can be configured in either whitelist mode or blacklist mode.
		When you enable system lockdown in default or whitelist mode, you block any application that is not on the approved applications list. When you enable system lockdown in blacklist mode, you block any application that is on the unapproved applications list.
		Note: Make sure that you test your configuration before you enable system lockdown. If you block a needed application, your client computers might be unable to restart.
		See "Making the blacklist mode for system lockdown appear in Symantec Endpoint Protection Manager" on page 503.
		See "Enabling system lockdown to run in whitelist mode" on page 517.
		See "Enabling system lockdown to run in blacklist mode" on page 518.

Table 22-6   System lockdown steps *(continued)*

Step	Action	Description
Step 7	Update file fingerprint lists for system lockdown	Over time, you might change the applications that run in your network. You can update your file fingerprint lists or remove lists as necessary.
		You can update file fingerprint lists in two ways:
		■ Manually import, append, replace, or merge file fingerprint lists. See "Manually updating a file fingerprint list in Symantec Endpoint Protection Manager" on page 507. See "Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager" on page 506.
		■ Automatically update existing file fingerprint lists when whitelist mode and blacklist mode are available. You can also automatically update applications on the application name lists that you import. See "Making the blacklist mode for system lockdown appear in Symantec Endpoint Protection Manager" on page 503. See "Automatically updating whitelists or blacklists for system lockdown" on page 509. See "Creating an application name list to import into the system lockdown configuration" on page 508.
		Note: You might want to re-test the entire system lockdown configuration if you add client computers to your network. You can move new clients to a separate group or test network where system lockdown is not enabled. Or you can keep system lockdown enabled and test individual file fingerprints or applications as described in the next step.
		See "Setting up and testing the system lockdown configuration before you enable system lockdown" on page 514.

Table 22-6   System lockdown steps *(continued)*

Step	Action	Description
Step 8	Test selected items before you add or remove them when system lockdown is enabled	After system lockdown is enabled, you can test individual file fingerprints, application name lists, or specific applications before you add or remove them to the system lockdown configuration.
		You might want to remove file fingerprint lists if you have many lists and no longer use some of them.
		Note: Be careful when you add or remove a file fingerprint list or a specific application from system lockdown. Adding or removing items from system lockdown can be risky. You might block important applications on your client computers.
		■ Test selected items. Use the **Test Before Removal** or **Test Before Addition** option to log specific file fingerprint lists or specific applications as unapproved. When you run this test, system lockdown is enabled but does not block any selected applications or any applications in the selected file fingerprint lists. Instead, system lockdown logs the applications as unapproved. ■ Check the Application Control log. The log entries appear in the Application Control log. If the log has no entries for the tested applications, then you know that your clients do not use those applications. You can safely remove the list.
		See "Testing selected items before you add or remove them when system lockdown is already enabled" on page 519.

See "Setting up application and device control" on page 482.

Making the blacklist mode for system lockdown appear in Symantec Endpoint Protection Manager

You can set up Symantec Endpoint Protection Manager so that system lockdown includes a blacklist option to block a specified list of unapproved applications. To use the blacklisting feature, you must modify the conf.properties file to let the blacklist mode option appear in the Symantec Endpoint Protection Manager console.

> **Note:** A whitelist mode is also available when the blacklist mode is available. Whitelist mode is the same as the default system lockdown functionality that lets only a list of approved applications that run on client computers.

You can specify a maximum number of named applications in the conf.properties file.

- By default, 512 is the maximum number. You should change the setting if you want to import a large number of application names into the system lockdown configuration in blacklist mode.

- The maximum number applies to the number of applications that you specify in your combined application name lists.

- The setting does not apply to file fingerprint lists, which have no maximum limitation on the number of applications that they include.

To make the blacklist mode for system lockdown appear in the Symantec Endpoint Protection Manager console

1   Stop the Symantec Endpoint Protection Manager service.

2   Open the conf.properties file with any text editor. The file is typically located in the C:\Program Files\Symantec\Symantec Endpoint Protection Manager\tomcat\etc folder.

3   To allow the new options to appear, add the following line to the file:

    ```
    scm.systemlockdown.blacklist.enabled=1
    ```

4   To specify a maximum number of applications to include in an application name list, add the following line to the file:

    ```
    scm.systemlockdown.max.count.extrafiles=max num of apps
    ```

5   Save the file.

6   Restart the Symantec Endpoint Protection Manager service.

See "Configuring system lockdown" on page 497.

See "Creating an application name list to import into the system lockdown configuration" on page 508.

See "Stopping and starting the management server service" on page 170.

Creating a file fingerprint list with checksum.exe

You can use the checksum.exe utility to create a file fingerprint list. The list contains the path and the file name and corresponding checksum for each executable file or DLL that resides in a specified path on the computer. The utility is installed with Symantec Endpoint Protection on the client computer.

You can also use a third-party utility to create a file fingerprint list.

You import the file fingerprint list into Symantec Endpoint Protection Manager to use in your system lockdown configuration.

See "Configuring system lockdown" on page 497.

The format of each line is *checksum_of_the_file* space *full_pathname_of_the_exe_or_DLL*.

An example of checksum.exe output is shown here:

```
0bb018fad1b244b6020a40d7c4eb58b7 c:\dell\openmanage\remind.exe
35162d98c2b445199fef95e838feae4b c:\dell\pnp\m\co\HSFCI008.dll
4f3ef8d2183f927300ac864d63dd1532 c:\dell\pnp\m\co\HXFSetup.exe
dcd15d648779f59808b50f1a9cc3698d c:\dell\pnp\m\co\MdmXSdk.dll
2f276c59243d3c051547888727d8cc78 c:\Nokia Video Manager\QtCore4.dll
e6b635b6f204b9f2a43ba7df8780a7a6 c:\Nokia Video Manager\QtNetwork4.dll
0901d37ec3339ef06dba0a9afb0ac97c c:\Nokia Video Manager\QtXml4.dll
a09eaad7f8c7c4df058bbaffd938cd4c c:\Nokia Video Manager\VideoManager.exe
```

To create a file fingerprint list with checksum.exe

1   Open a command prompt window on the computer that contains the image for which you want to create a file fingerprint list.

    The computer must have Symantec Endpoint Protection client software installed.

2   Navigate to the folder that contains the file checksum.exe. By default, this file is located in the following folder:

    C:\Program Files\Symantec\Symantec Endpoint Protection

3   Type the following command:

    ```
    checksum.exe outputfile path
    ```

    where *outputfile* is the name of the text file that contains the checksums for all the applications that are located on the specified drive. The output file is a text file (*outputfile.txt*).

The following is an example of the syntax you could use to create a fingerprint list for an image:

```
checksum.exe cdrive.txt c:
```

This command creates a file that is called cdrive.txt. It contains the checksums and file paths of all the executables and DLLs found on the C drive of the client computer on which it was run.

The following is an example of the syntax that you could use to create a fingerprint for a folder on the client computer:

```
checksum.exe blocklist.txt c:\Files
```

This command creates a file that is called blocklist.txt. It contains the checksums and file paths of any executables and DLLs found in the Files folder.

Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager

Before you can use a file fingerprint list in system lockdown, you must import the file into Symantec Endpoint Protection Manager. You can also merge file fingerprint lists.

You must have created the file fingerprint list already. You can use the checksum.exe utility or a third-party utility to create the file fingerprint list.

See "Configuring system lockdown" on page 497.

See "Creating a file fingerprint list with checksum.exe" on page 505.

Importing or merging file fingerprint lists

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

2   Under **Policies**, expand **Policy Components**, and then click **File Fingerprint Lists**.

3   Under **Tasks**, click **Add a File Fingerprint List**.

4   In the **Welcome to the Add File Fingerprint Wizard**, click **Next**.

5   In the **Information about New File Fingerprint** panel, type a name and description for the new list.

6   Click **Next**.

7   In the **Create a File Fingerprint** panel, select one of the following options:

■ **Create the file fingerprint by importing a file fingerprint file**

■ **Create the file fingerprint by combining multiple existing file fingerprints**
This option is only available if you have already imported multiple file fingerprint lists.

8   Click **Next**.

9   Do one of the following actions:

   ■ Specify the path to the file fingerprint that you created. You can browse
      to find the file.

   ■ Select the fingerprint lists that you want to merge.

10 Click **Next**.

11 Click **Close**.

12 Click **Finish**.

   The imported or merged fingerprint list appears under **File Fingerprint Lists**.

Manually updating a file fingerprint list in Symantec Endpoint Protection Manager

You might want to update your file fingerprint lists after you run system lockdown
for a while. You can append, replace, or remove entries in an existing file
fingerprint list. You cannot directly edit an existing file fingerprint list in Symantec
Endpoint Protection Manager.

Note: You can also export an existing file fingerprint list.

If you want to merge fingerprint lists into a new list with a different name, use
the **Add a File Fingerprint Wizard**.

See "Importing or merging file fingerprint lists in Symantec Endpoint Protection
Manager" on page 506.

See "Configuring system lockdown" on page 497.

To update a file fingerprint list in Symantec Endpoint Protection Manager

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

2   Under **Policies**, expand **Policy Components**, and then click **File Fingerprint
   Lists**.

3   In the **File Fingerprint Lists** pane, select the fingerprint list that you want
   to edit.

4   Click **Edit**.

5   In the **Edit File Fingerprint Wizard**, click **Next**.

6   Do one of the following:

- Click **Append a fingerprint file to this file fingerprint** to add a new file to an existing one.

- Click **Append another file fingerprint to this file fingerprint** to merge file fingerprint lists that you already imported.

- Click **Replace an existing list with a new file fingerprint list**.

- Click **Remove fingerprints from an existing list that match fingerprints in a new list**.

7   Do one of the following:

- Click **Browse** to locate the file or type the full path of the file fingerprint list that you want to append, replace, or remove.

- Select the file fingerprints that you want to merge.

8   Click **Next**.

9   Click **Close**.

10 Click **Finish**.

Creating an application name list to import into the system lockdown configuration

You can import a list of application names into the system lockdown configuration when blacklist mode is available. You might want to import an application name list rather than adding application names individually to the system lockdown configuration.

By default, 512 is the maximum number of applications that you can include in your combined application name lists. You can change the maximum in the conf.properties file.

You can create an application name list file with any text editor.

Each line of the file can contain the following items each separated by a space:

- The file name
  If you use a path name, it must be in quotes.

- The test mode
  The value should be 1 or Y for enabled or 0 or N for disabled. If you leave the field blank, test mode is disabled. You must include a value if you want to specify the matching mode.

- The matching mode (wildcard or regular expression)
  The value should be 1or Y for regular expression matching or 0 or N for wildcard matching. If you leave the field blank, wildcard matching is used.

Note: The test mode field enables or disables the **Test Before Addition** or **Test Before Removal** option for each application in the list. The test mode field is ignored when you use the **Log Applications Only** option to test the entire system lockdown configuration.

Each line should use the following syntax:

```
filename test_mode matching_mode
```

For example:

```
aa.exe
bb.exe 0 1
cc.exe 1
dd.exe 1 0
"c:\program files\ee.exe" 0 0
```

When you import this list into system lockdown, the individual applications appear in the system lockdown configuration with the following settings:

Table 22-7   Example matching mode settings

Application Name	Test Before Addition or Test Before Removal	Matching Mode
aa.exe	Disabled	Wildcard
bb.exe	Disabled	Regular expression
cc.exe	Enabled	Wildcard
dd.exe	Enabled	Wildcard
c:\program files\ee.exe	Disabled	Wildcard

See "Making the blacklist mode for system lockdown appear in Symantec Endpoint Protection Manager" on page 503.

See "Configuring system lockdown" on page 497.

Automatically updating whitelists or blacklists for system lockdown

Symantec Endpoint Protection Manager can automatically update existing file fingerprint lists and application name lists that system lockdown uses in whitelist or blacklist mode.

Symantec Endpoint Protection Manager can update existing lists. It cannot automatically upload a new whitelist or blacklist.

You can also manually update existing file fingerprints.

Table 22-8   Updating whitelists or blacklists for system lockdown

Step	Task	Description
Step 1	Create updated file fingerprint lists or application name lists and compress the files	You can use the checksum.exe utility or any third-party utility to create the updated file fingerprint lists. You can use any text editor to update application name lists. The lists must have the same names that already exist in Symantec Endpoint Protection Manager. See "Creating a file fingerprint list with checksum.exe" on page 505. The automatic updates feature requires a compressed file (zip file) of the file fingerprint and application name lists. You can use the file compression feature in Windows or any compression utility to zip the files.
Step 2	Create an index.ini file	The index.ini file specifies which file fingerprint lists and application names lists Symantec Endpoint Protection Manager should update. You can create an index.ini file with any text editor and copy the file to the specified URL. See "Creating an index.ini file for automatic updates of whitelists and blacklists that are used for system lockdown" on page 511.
Step 3	Make the compressed file and index.ini available to Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager uses UNC, FTP, or HTTP/HTTPS to retrieve the index.ini file and zip file at the specified URL. Symantec Endpoint Protection Manager uses the instructions in the index.ini file to update the specified files. When you enable automatic updates, Symantec Endpoint Protection Manager periodically checks the URL for updated files based on the schedule you set. **Note:** If you cannot use UNC, FTP, or HTTP/HTTPS, you can copy the index.ini and updated file fingerprint and application name files directly into the following folder: ..\Symantec Endpoint Protection Manager\data\inbox\WhitelistBlacklist\content. The files should be unzipped. Symantec Endpoint Protection Manager checks this folder if it cannot use UNC, FTP, or HTTP/HTTPS to update the files.

Step	Task	Description
Step 4	Enable automatic whitelist and blacklist updates in the management console	You must enable the automatic update of existing whitelists or blacklists in the Symantec Endpoint Protection Manager console.
		You use the **File Fingerprint Update** dialog in Symantec Endpoint Protection Manager to enable the update feature and specify the schedule and the URL information. The blacklist mode must be available in Symantec Endpoint Protection Manager.
		See "Making the blacklist mode for system lockdown appear in Symantec Endpoint Protection Manager" on page 503.
		See "Enabling automatic updates of whitelists and blacklists for system lockdown" on page 513.
Step 5	Check the status of automatic updates for the whitelist or blacklist	You can make sure that Symantec Endpoint Protection Manager completes the updates by checking the status in the console.
		See "Checking the status of automatic whitelist or blacklist updates for system lockdown" on page 513.

See "Manually updating a file fingerprint list in Symantec Endpoint Protection Manager" on page 507.

See "Configuring system lockdown" on page 497.

Creating an index.ini file for automatic updates of whitelists and blacklists that are used for system lockdown

The automatic updates feature requires an index.ini file. You can create the file with any text editor.

Note: If you use non-English characters in the text file, you should use UTF-8 without a byte order mark (BOM) character to edit and save the file.

The index.ini file specifies the following items:

■ The revision and name of the compressed file that includes your updated file fingerprint lists and application name lists.

■ The names of the file fingerprint lists and application name lists that you want to update.

■ The names of the client groups that use the application name lists.

The existing file fingerprint list or group must currently exist in Symantec Endpoint Protection Manager. The group must have system lockdown enabled.

The file fingerprint lists and application name lists must be available in the specified compressed file.

You must structure the index.ini file with the following syntax:

```
[Revision]
Revision=YYYYMMDD RXXX
SourceFile=zip file name
Description=optional description

[FingerprintList - domain name or Default]
existing fingerprint list="updated list" REPLACE/APPEND/REMOVE


[ApplicationNameList - domain name or Default]
existing group path="updated list" REPLACE/APPEND/REMOVE
```

For example, you could use the following lines in an index.ini file:

```
[Revision]
Revision=20111014 R001
SourceFile=20110901 R001.zip
Description=NewUpdates

[FingerprintList - Default]
FingerprintListName 1="FingerprintList1.txt" REPLACE
FingerprintListName 2="FingerprintList2.txt" REPLACE

[ApplicationNameList - Default]
My Company\Group AA\Group AA 1="ApplicationNameList1.txt" REPLACE
My Company\Group AA\Group AA 2="ApplicationNameList2.txt" REPLACE

[FingerprintList - DomainABC]
FingerprintListName 1="FingerprintList1.txt" REPLACE
FingerprintListName 2="FingerprintList2.txt" REPLACE

[ApplicationNameList - DomainABC]
My Company\Group AA\Group AA 1="ApplicationNameList1.txt" REPLACE
My Company\Group AA\Group AA 2="ApplicationNameList2.txt" REPLACE
```

See "Automatically updating whitelists or blacklists for system lockdown" on page 509.

See "Creating an application name list to import into the system lockdown configuration" on page 508.

Enabling automatic updates of whitelists and blacklists for system lockdown

You can automatically update whitelists and blacklists that you use for system lockdown.

To enable automatic whitelist and blacklist updates in the management console

1   In the console, on the **Admin** tab, click **Servers**.

2   Right-click the relevant server, and select **Edit the server properties**.

3   In the **Server Properties** dialog box, select the **File Fingerprint Update** tab.

The tab appears only if you have configured the console to run whitelist and blacklist mode by setting scm.systemlockdown.blacklist.enabled=1 in the conf.properties file.

4   On the **File Fingerprint Update** tab, check **Automatically update the whitelist or blacklist**.

5   Enter the URL for the location of the index.ini and the compressed file.

If you want to use UNC or FTP, you must also specify a user name and password for both the index.ini and the content.

6   Under **Schedule**, you can specify how often Symantec Endpoint Protection Manager should try to update the whitelist or blacklist or you can use the default setting.

7   Click **OK**.

Checking the status of automatic whitelist or blacklist updates for system lockdown

After Symantec Endpoint Protection Manager updates a whitelist or blacklist, you can check the status of the update in several ways.

To check the status of automatic whitelist or blacklist updates for system lockdown

◆   In the console, do one of the following actions:

■   On the **Admin** tab, select the site. A message appears similar to the following message: **Update whitelist and blacklist for revision 20120528 R016** *description* **succeeded**.

■ On the **Monitors** tab, view **System Logs: Server Activity**. The event type typically appears similar to **File fingerprint update**.

■ On the **Policies** tab, under **Policy Components**, check the file fingerprint list description. The description appears similar to **Revision: 20120528 R016** *description*.

See "Automatically updating whitelists or blacklists for system lockdown" on page 509.

See "Viewing logs" on page 624.

Setting up and testing the system lockdown configuration before you enable system lockdown

Typically, you run system lockdown in test mode for a week, or enough time for clients to run their typical applications. After you determine that your system lockdown settings do not cause problems for users, you can enable system lockdown.

When you run system lockdown in test mode, system lockdown is disabled. System lockdown does not block any applications. Instead, unapproved applications are logged rather than blocked so that you can review the list before you enable system lockdown. You can view the log entries in the Control log. You can also view the unapproved applications in the **System Lockdown** dialog box.

Note: You can also create firewall rules to allow approved applications on the client.

To set up and test the system lockdown configuration before you enable system lockdown

1   In the console, click **Clients**, then under **Clients,** locate the group for which you want to set up system lockdown.

2   On the **Policies** tab, click **System Lockdown**.

3   In the **System Lockdown for** *name of group* dialog box, if you configured the console to show the mode, select **Enable Whitelist Mode** or **Enable Blacklist Mode**.

See "Making the blacklist mode for system lockdown appear in Symantec Endpoint Protection Manager" on page 503.

4 Click **Step 1: Log Unapproved Applications Only** to run system lockdown in test mode.

This option logs the unapproved applications that clients are currently running.

5 Do one of the following:

- Under **Approved Applications**, under **File Fingerprint List**, add or remove file fingerprint lists.

- Under **Unapproved Applications**, under **File Fingerprint List** add or remove file fingerprint lists.

To add a list, the list must be imported and available in Symantec Endpoint Protection Manager.

See "Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager" on page 506.

6 To add applications from a list of applications, do one of the following:

- Under **Approved Applications**, under **File Name**, click **Import** to add an application name list.

- Under **Unapproved Applications**, under **File Name**, click **Import** to add an application name list.

Specify the application name list that you want to import and click **Import**. The applications in the list appear as individual entries in the system lockdown configuration.

Note: The import option is only available if blacklist mode is available. The application name list must be a text file that specifies the file name, test mode, and matching mode.

See "Creating an application name list to import into the system lockdown configuration" on page 508.

7 To add an individual application, do one of the following.

- Under **Approved Applications**, under **File Name**, click **Add** to add an individual application.

- Under **Unapproved Applications**, under **File Name**, click **Add** to add an individual application.

8   In the **Add File Definition** dialog box, specify the full path name of the file
     (.exe or .dll).

     Names can be specified using a normal string or regular expression syntax.
     Names can include wildcard characters (* for any characters and ? for one
     character). The name can also include environment variables such as
     %ProgramFiles% to represent the location of your Program Files directory
     or %windir% for the Windows installation directory.

9   Either leave **Use wildcard matching (* and ? supported)** selected by default,
     or click **Use regular expression matching** if you used regular expressions in
     the file name instead.

10   If you want to allow the file only when it is executed on a particular drive
     type, click **Only match files on the following drive types**.

     Unselect the drive types you do not want to include. By default, all drive types
     are selected.

11   If you want to match by device ID type, check **Only match files on the
     following device id type**, and then click **Select**.

12   Click the device you want in the list, and then click **OK**.

13   Click **OK** to start the test.

After a period of time, you can view the list of unapproved applications. If you
re-open the **System Lockdown for *name of group*** dialog box, you can see how
long the test has been running.

To view the unapproved applications that the test logged but did not block

1   In the **System Lockdown *name of group*** dialog box, click **View Unapproved
     Applications**.

2   In the **Unapproved Applications** dialog box, review the applications.

     This list includes information about the time that the application was run,
     the computer host name, the client user name, and the executable file name.

3   Determine how you want to handle the unapproved applications.

     For whitelist mode, you can add the names of applications that you want to
     allow to the list of approved applications. For blacklist mode, you can remove
     the names of applications that you want to allow.

4   In the **Unapproved Applications** dialog, click **Reset the Test** if you changed
     the file fingerprint lists or individual applications and want to run the test
     again. Otherwise, click **Close**.

5   After you finish testing, you can enable system lockdown.

See "Configuring system lockdown" on page 497.

Enabling system lockdown to run in whitelist mode

You can enable system lockdown to allow only approved applications on your client computers. Only applications in the approved list are allowed to run. All other applications are blocked. The approved list is called a whitelist. Approved applications are subject to Symantec Endpoint Protection's other protection features.

Note: By default, system lockdown runs in whitelist mode when you enable it. You can choose a whitelist or blacklist mode if you set up Symantec Endpoint Protection Manager to show both options.

You should configure system lockdown to run in whitelist mode only after the following conditions are true:

■ You tested the system lockdown configuration with the **Log Unapproved Applications Only** option.

■ You are sure that all the applications that your client computers need to run are listed in the approved applications list.

To enable system lockdown to run in whitelist mode

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

2 Under **Clients**, select the group for which you want to set up system lockdown.

 If you select a subgroup, the parent group must have inheritance turned off.

3 On the **Policies** tab, click **System Lockdown**.

4 If you configured Symantec Endpoint Protection Manager to display the whitelist and blacklist mode options, click **Enable Whitelist Mode**.

5 Click **Step 2: Enable System Lockdown** to block any unapproved applications that clients try to run.

6 Under **Approved Applications**, make sure that you have included all the applications that your client computers run.

Warning: You must include all the applications that your client computers run in the approved applications list. If you do not, you could make some client computers unable to restart or prevent users from running important applications.

---

7 To display a message on the client computer when the client blocks an application, check **Notify the user if an application is blocked**.

8 Click **OK**.

See "Making the blacklist mode for system lockdown appear in Symantec Endpoint Protection Manager" on page 503.

See "Setting up and testing the system lockdown configuration before you enable system lockdown" on page 514.

See "Configuring system lockdown" on page 497.

See "Disabling and enabling a group's inheritance" on page 218.

Enabling system lockdown to run in blacklist mode

You can enable system lockdown to block a list of unapproved applications on your client computers. All applications in the unapproved list are blocked. The unapproved list is called a blacklist. Any other applications are allowed. Allowed applications are subject to Symantec Endpoint Protection's other protection features.

Note: You can choose the whitelist or blacklist mode if you set up Symantec Endpoint Protection Manager to show both options.

You should configure system lockdown to block unapproved applications only after the following conditions are true:

- You tested the system lockdown configuration with the **Log Unapproved Applications Only** option.

- You are sure that all of the applications that your client computers should block are listed in the unapproved applications list.

To enable system lockdown to run in blacklist mode

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

2 Under **Clients**, select the group for which you want to set up system lockdown.

If you select a subgroup, the parent group must have inheritance turned off.

See "Disabling and enabling a group's inheritance" on page 218.

3 On the **Policies** tab, select **System Lockdown**.

4 In the **System Lockdown** dialog box, select **Enable Blacklist Mode**.

5   Click **Step 2: Enable System Lockdown**. This step blocks any unapproved
    applications that clients try to run on the client computers in the selected
    group.

6   Under **Unapproved Applications**, make sure that you have included all the
    applications that your client computers should block.

Note: A large number of named applications might decrease your client
computer performance.

---

7   To display a message on the client computer when the client blocks an
    application, check **Notify the user if an application is blocked**.

8   Click **OK**.

See "Making the blacklist mode for system lockdown appear in Symantec Endpoint
Protection Manager" on page 503.

See "Setting up and testing the system lockdown configuration before you enable
system lockdown" on page 514.

See "Configuring system lockdown" on page 497.

Testing selected items before you add or remove them when system lockdown is already enabled

After system lockdown is enabled for a period of time, you might want to add or
remove file fingerprint lists or specific applications. Over time you might
accumulate many file fingerprint lists that you no longer use. Or the applications
that your users need might change.

You test specific items before you add or remove them so that your client
computers do not block important applications. In blacklist mode, system lockdown
blocks any new items that you add to the configuration. In whitelist mode, system
lockdown blocks any existing items that you remove. System lockdown runs in
whitelist mode by default. The modes only appear as options in the console if you
configure the console to show the options.

Note: When you test individual items, system lockdown is enabled. System
lockdown continues to block the applications that are not part of the test.

You can test individual file fingerprint lists to make sure that your client computers
no longer use the applications in the list. You can also test the individual
applications that are specified in the system lockdown configuration.

You can test the entire system lockdown configuration, rather than specific items, when system lockdown is disabled.

To test selected items before you add or remove them when system lockdown is already enabled

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

2   Under **Clients**, locate the group for which you want to remove items from system lockdown.

3   On the **Policies** tab, click **System Lockdown**.

The system lockdown configuration should already be enabled.

- For whitelist mode, you should know which existing file fingerprint list or the specific application name that you want to test.

- For blacklist mode you should add a new file fingerprint list or application name that you want to test.

See "Enabling system lockdown to run in whitelist mode" on page 517.

See "Enabling system lockdown to run in blacklist mode" on page 518.

4   Do one of the following:

- In whitelist mode, under **Approved Applications**, check **Test Before Removal** next to an existing file fingerprint list or application that you want to test.

- In blacklist mode, under **Unapproved Applications**, check **Test Before Addition** next to a new file fingerprint list or application that you want to test.

System lockdown continues to allow these applications, but they are logged as unapproved applications.

If you imported an application name list, the **Test Before Removal** or **Test Before Addition** field is already populated.

5   Click **OK** to start the test.

If you re-open the **System Lockdown for *name of group*** dialog box, you can see how long the test has been running. Typically, you might want to run this test for a week or more.

After the test, you can check the Application Control log. If the applications that you tested appear in the Application Control log, you know that your users run the applications. You can decide whether to keep the tested item as part of the system lockdown configuration.

If you decide that you now want to block the items that you tested, do one of the following actions:

- In the **System Lockdown for** *name of group* dialog box, when whitelist mode is enabled, select the tested item and click **Remove**.

- In the **System Lockdown for** *name of group* dialog box, when blacklist mode is enabled, unselect **Test Before Addition**.

Warning: In whitelist mode, system lockdown blocks any applications on file fingerprint lists and the specific application names that you remove from the configuration. In blacklist mode, system lockdown blocks any applications on file fingerprint lists and the specific application names that you add to the configuration.

See "Setting up and testing the system lockdown configuration before you enable system lockdown" on page 514.

See "Configuring system lockdown" on page 497.

See "Making the blacklist mode for system lockdown appear in Symantec Endpoint Protection Manager" on page 503.

Managing device control

You use the hardware devices list and an Application and Device Control policy to manage device control.

See "Setting up application and device control" on page 482.

See "About application and device control" on page 479.

See "About Application and Device Control policies" on page 481.

Table 22-9   Managing device control

Action	Description
Review the default hardware devices list in Symantec Endpoint Protection Manager	By default, Symantec Endpoint Protection Manager includes a list of hardware devices. The list appears on the **Policies** tab in Symantec Endpoint Protection Manager under **Policy Components**. You use this list to select the devices that you want to control on your client computers.
	If you want to control a device that is not included in the list, you must add the device first.
	See "About the hardware devices list" on page 522.

Table 22-9   Managing device control *(continued)*

Action	Description
Add devices to the hardware devices list (if necessary)	When you add a device to the device list, you need a class ID or device ID for the device. See "Adding a hardware device to the Hardware Devices list" on page 524. See "Obtaining a class ID or device ID" on page 523.
Configure device control	Specify the devices that you want to block or exclude from blocking. See "Configuring device control" on page 525.

About the hardware devices list

Symantec Endpoint Protection Manager includes a hardware devices list. Some devices are included in the list by default. You use the devices when you configure device control.

See "Managing device control" on page 521.

You can add devices to the list. You cannot edit or delete any default devices.

Devices are identified by a device ID or class ID. You use either of these values to add a device to the list.

See "Obtaining a class ID or device ID" on page 523.

class ID	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}

device ID	A device ID is the most specific ID for a device. The syntax of a device ID includes some descriptive strings that make it easier to read than the class ID.
	When you add a device ID, you can use a device's specific ID. Alternately, you can use a wildcard character in the device ID string to indicate a less specific group of devices. You can use an asterisk (*) to indicate zero or more additional characters or a question mark (?) to indicate a single character of any value.
	The following is a device ID for a specific USB SanDisk device:
	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO&REV_2033 \0002071406&0
	The following is a device ID with a wildcard that indicates any USB SanDisk device:
	USBSTOR\DISK&VEN_SANDISK*
	The following is a device ID with a wildcard that indicates any USB disk device:
	USBSTOR\DISK*
	The following is a device ID with a wildcard that indicates any USB storage device:
	USBSTOR*

Obtaining a class ID or device ID

You can use the Symantec DevViewer tool to obtain either the class ID (GUID) or the device ID. You can use Windows Device Manager to obtain the device ID.

After you obtain a device ID, you can modify it with a wildcard character to indicate a less specific group of devices.

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

1 On the Tools product disc, locate the `\Tools\DevViewer` folder, and then download the `DevViewer.exe` tool to the client computer.

2 On the client computer, run `DevViewer.exe`.

3 Expand the Device Tree and locate the device for which you want the device ID or the GUID.

For example, expand DVD-ROM drives and select the device within that category.

4 In the right-hand pane, right-click the device ID (which begins 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 Open the Device Manager from the Control Panel.

The path to the Device Manager depends on the Windows operating system. For example, in Windows 7, click **Start > Control Panel > System > Device Manager**.

2 In the **Device Manager** dialog box, right-click the device, and click **Properties**.

3 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.

4 Copy the ID string.

5 Click **OK**.

See "Adding a hardware device to the Hardware Devices list" on page 524.

Adding a hardware device to the Hardware Devices list

After you obtain a class ID or device ID for a hardware device, you can add the hardware device to the default Hardware Devices list. You can then access this default list from the device control part of the Application and Device Control policy.

See "About the hardware devices list" on page 522.

To add hardware devices to the Hardware Devices list

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

2 Under **Policies**, expand **Policy Components** and click **Hardware Devices**.

3 Under **Tasks**, click **Add a Hardware Device**.

4 Enter the name of the device you want to add.

Both Class IDs and Device IDs are enclosed in curly braces by convention.

5 Select either **Class ID** or **Device ID**, and paste the ID that you copied from the Windows Device Manager or the DevViewer tool.

6   You can use wildcard characters to define a set of device IDs. For example,
     you can use the following string: `*IDE\DVDROM*`.

     See "Obtaining a class ID or device ID" on page 523.

7   Click **OK**.

Configuring device control

You use an Application and Device Control policy to configure device control. You
have already added any devices you need to the Hardware Devices list.

See "Managing device control" on page 521.

See "About application and device control" on page 479.

Configuring device control

1   In the console, open an Application and Device Control policy.

2   Click **Device Control**.

3   Under **Blocked Devices**, click **Add**.

4   In the **Device Selection** window, select one or more devices. Make sure that
     if you block ports that you exclude devices if necessary.

     Note: Typically, you should never block a keyboard.

     ---

5   Click **OK**.

6   Under **Devices Excluded From Blocking**, click **Add**.

7   In the **Device Selection** window, select one or more devices.

8   Check **Notify users when devices are blocked** if you want to notify the user.

9   Click **Specify Message Text** to type the message that appears in the
     notification.

10   Click **OK**.

Managing exceptions

This chapter includes the following topics:

- About exceptions to Symantec Endpoint Protection
- Managing exceptions for Symantec Endpoint Protection
- Creating exceptions for Symantec Endpoint Protection
- Restricting the types of exceptions that users can configure on client computers
- Creating exceptions from log events in Symantec Endpoint Protection Manager

About exceptions to Symantec Endpoint Protection

Typically exceptions are items, such as files or Web domains, that you want to exclude from scans.

Symantec Endpoint Protection automatically excludes some files from virus and spyware scans.

You can also use exceptions to detect an application or to change the default behavior when Symantec Endpoint Protection detects an application or when the application launches.

You might want to use exceptions to reduce the amount of time that scans run. For example, you can exclude files, folders, and extensions from scans. If you reduce the scan time, you might increase the system performance on client computers.

Note: You cannot create exceptions for an individual virus and spyware scans. For example, if you create a file exception, Symantec Endpoint Protection applies the exception to all virus and spyware scans (Auto-Protect, Download Insight, and any administrator-defined or user-defined scan).

Exceptions apply to a particular client type (Windows or Mac). You configure the exceptions separately. For example, if you configure a file exception, it applies either to clients that run on Windows computers or clients that run on Mac computers. Some exceptions are not available for Mac clients.

Table 23-1   Scan exceptions and client type

Client Type	Exception
Mac clients	File or folder exception
Windows clients	You can configure the following types of exceptions: ■ File ■ Folder ■ Known risk ■ Extension ■ Trusted Web domain ■ Application to monitor ■ Application ■ Tamper Protection

See "About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans" on page 332.

See "Managing exceptions for Symantec Endpoint Protection" on page 528.

Managing exceptions for Symantec Endpoint Protection

You can manage exceptions for Symantec Endpoint Protection in the Symantec Endpoint Protection Manager console.

Table 23-2   Managing exceptions

Task	Description
Learn about exceptions	You use exceptions to exclude items from scans and protection on your client computers. See "About exceptions to Symantec Endpoint Protection" on page 527.

Table 23-2   Managing exceptions *(continued)*

Task	Description
Review the types of files and folders that Symantec Endpoint Protection automatically excludes from scans	Symantec Endpoint Protection automatically creates exceptions, or exclusions, for some third-party applications and some Symantec products. You can also configure individual scans to scan only certain extensions and skip any other extensions. See "About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans" on page 332.
Create exceptions for scans	You add exceptions in an Exceptions policy directly. Or you can add exceptions from log events on the **Monitors** page. See "Creating exceptions for Symantec Endpoint Protection" on page 530. See "Creating exceptions from log events in Symantec Endpoint Protection Manager" on page 541.
Restricting the types of exceptions that users can configure on client computers	By default, users on client computers have limited configuration rights for exceptions. You can restrict users further so that they cannot create exceptions for virus and spyware scans or for SONAR. Users can never force an application detection and they never have permission to create Tamper Protection exceptions. Users also cannot create a file exception for application control. See "Restricting the types of exceptions that users can configure on client computers" on page 541.

Table 23-2   Managing exceptions *(continued)*

Task	Description
Check the logs for detections for which you might want to create exceptions	After Symantec Endpoint Protection makes a detection, you can create an exception for the detection from the log event.
	For example, you might want to create an exception for a file that scans detect but that your users request to download.
	See "Creating exceptions from log events in Symantec Endpoint Protection Manager" on page 541.
Configure intrusion prevention exceptions	You can specify exceptions for intrusion prevention.
	You can also set up a list of excluded hosts for intrusion prevention.
	Intrusion prevention exceptions are configured in an Intrusion Prevention policy.
	See "Managing intrusion prevention on your client computers" on page 461.

Creating exceptions for Symantec Endpoint Protection

You can create different types of exceptions for Symantec Endpoint Protection.

Any exception that you create takes precedence over any exception that a user might define. On client computers, users cannot view the exceptions that you create. A user can view only the exceptions that the user creates.

Note: The Exceptions policy includes a SONAR file path exception to prevent SONAR code injection into the specified application. SONAR does not inject code into applications on Symantec Endpoint Protection 12.1 or earlier clients. If you use Symantec Endpoint Protection Manager 12.1.2 to manage clients, a SONAR file exception in an Exceptions policy is ignored on your legacy clients. If you use a legacy Symantec Endpoint Protection Manager to manage clients, the legacy policy does not support SONAR file exceptions for your Symantec Endpoint Protection 12.1.2 clients. You can prevent SONAR code injection into applications on these clients, however, by creating an **Application to monitor** exception in the legacy policy. After the client learns the application, you can configure an application exception in the policy.

Exceptions for virus and spyware scans also apply to Download Insight.

Table 23-3   Creating exceptions for Symantec Endpoint Protection

Task	Description
Exclude a file from scans	Supported on Windows and Mac clients.
	Excludes a file by name from virus and spyware scans, SONAR, or application control on Windows clients.
	You can also exclude a file from virus and spyware scans on Mac clients.
	See "Excluding a file or a folder from scans" on page 534.
Exclude a folder from scans	Supported on Windows and Mac clients.
	Excludes a folder from virus and spyware scans, SONAR, or all scans on Windows clients. You can also exclude a folder from virus and spyware scans on Mac clients.
	See "Excluding a file or a folder from scans" on page 534.
Exclude a known risk from virus and spyware scans	Supported on Windows clients.
	Excludes a known risk from virus and spyware scans. The scans ignore the risk, but you can configure the exception so that the scans log the detection. In either case, the client software does not notify users when it detects the specified risks.
	If a user configures custom actions for a known risk that you configure to ignore, Symantec Endpoint Protection ignores the custom actions.
	See "Excluding known risks from virus and spyware scans" on page 536.
	Security risk exceptions do not apply to SONAR.
Exclude file extensions from virus and spyware scans	Supported on Windows clients.
	Excludes any files with the specified extensions from virus and spyware scans.
	See "Excluding file extensions from virus and spyware scans" on page 536.
	Extension exceptions do not apply to SONAR.

| | Table 23-3 | Creating exceptions for Symantec Endpoint Protection *(continued)* |

Task	Description
Monitor an application to create an exception for the application	Supported on Windows clients. Use the **Application to monitor** exception to monitor a particular application. When Symantec Endpoint Protection learns the application, you can create an exception to specify how Symantec Endpoint Protection handles the application. If you disable application learning, the Application to monitor exception forces application learning for the application that you specify. See "Monitoring an application to create an exception for the application" on page 537.
Specify how scans handle monitored applications	Supported on Windows clients. Use an application exception to specify an action for Symantec Endpoint Protection to apply to a monitored application. The type of action determines whether Symantec Endpoint Protection applies the action when it detects the application or when the application runs. Symantec Endpoint Protection applies the Terminate, Quarantine, or Remove action to an application when it launches or runs. It applies the Log only or Ignore action when it detects the application. Unlike a file name exception, an application exception is a hash-based exception. Different files can have the same name, but a file hash uniquely identifies an application. The application exception is a SHA-2 hash-based exception. Legacy exceptions for TruScan proactive threat scans appear as SHA-1 hash-based exceptions. Legacy clients support SHA-1 exceptions only. The file fingerprint in the exceptions list is preceded by a 2 or a 1 respectively to indicate the file hash type. Applications for which you can create exceptions appear in the **Exceptions** dialog after Symantec Endpoint Protection learns the application. You can request that Symantec Endpoint Protection monitors a specific application to learn. See "Specifying how Symantec Endpoint Protection handles monitored applications" on page 537. See "Configuring the management server to collect information about the applications that the client computers run" on page 313.

Table 23-3	Creating exceptions for Symantec Endpoint Protection *(continued)*

Task	Description
Exclude a Web domain from scans	Supported on Windows clients. Download Insight scans the files that users try to download from Web sites and other portals. Download Insight runs as part of a virus and spyware scan. You can configure an exception for a specific Web domain that you know is safe. Download Insight must be enabled for the exception to have any effect. **Note:** If your client computers use a proxy with authentication, you must specify trusted Web domain exceptions for Symantec URLs. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites. See the following related knowledge base articles: ■ How to test connectivity to Insight and Symantec licensing servers ■ Required exclusions for proxy servers to allow Symantec Endpoint Protection to connect to Symantec reputation and licensing servers See "Excluding a trusted Web domain from scans" on page 538.
Create file exceptions for Tamper Protection	Supported on Windows clients. Tamper Protection protects client computers from the processes that tamper with Symantec processes and internal objects. When Tamper Protection detects a process that might modify the Symantec configuration settings or Windows registry values, it blocks the process. Some third-party applications inadvertently try to modify Symantec processes or settings. You might need to allow a safe application to modify Symantec settings. You might want to stop Tamper Protection for certain areas of the registry or certain files on the client computer. In some cases, Tamper Protection might block a screen reader or some other assistive technology application. You can create a file exception so that the application can run on client computers. Folder exceptions are not supported for Tamper Protection. See "Creating a Tamper Protection exception" on page 539.
Allow applications to make DNS or host file changes	Supported on Windows clients You can create an exception for an application to make a DNS or host file change. SONAR typically prevents system changes like DNS or host file changes. You might need to make an exception for a VPN application, for example. See "Creating an exception for an application that makes a DNS or host file change" on page 540.

See "Managing exceptions for Symantec Endpoint Protection" on page 528.

See "Creating exceptions from log events in Symantec Endpoint Protection Manager" on page 541.

Excluding a file or a folder from scans

You add exceptions for files or folders individually. If you want to create exceptions for more than one file, repeat the procedure.

You can configure file or folder exceptions on both Windows and Mac clients. On Windows clients, file exceptions can apply to virus and spyware scans, SONAR, and application control. Folder exceptions apply to virus and spyware scans and SONAR.

To exclude a file from scans on Windows clients

1 On the **Exceptions Policy** page, click **Exceptions**.

2 Under **Exceptions**, click **Add > Windows Exceptions > File**

3 In the **Prefix variable** drop-down box, select a common folder.

   Select **[NONE]** to enter the absolute path and file name.

   When you select a prefix, the exception can be used on different Windows operating systems.

4 In the **File** text box, type the name of the file.

   If you select a prefix variable, the path should be relative to the prefix. If you select **[NONE]**, type the full path name.

   Note: Paths must be denoted by using a backward slash.

   ---

5 Under **Specify the types of scans that will exclude this file**, select the type of scan (**Security Risk**, **SONAR**, or **Application control**).

   You must select at least one type.

6 For security risk scans, under **Specify the type of security risk scan**, select **Auto-Protect**, **Scheduled and on-demand**, or **All Scans**.

7 Click **OK**.

To exclude a folder from scans on Windows clients

1 On the **Exceptions Policy** page, click **Exceptions**.

2 Under **Exceptions**, click **Add > Windows Exceptions > Folder**

3   In the **Prefix variable** drop-down box, select a common folder.

Select **[NONE]** to enter the absolute path and file name.

When you select a prefix, the exception can be used on different Windows operating systems.

4   In the **Folder** text box, type the name of the folder.

If you select a prefix variable, the path should be relative to the prefix. If you select **[NONE]**, type the full path name.

Note: Paths must be denoted by using a backward slash.

---

5   Under **Specify the type of scan that excludes this folder**, select the type of scan (**Security Risk**, **SONAR**, **Application control**, or **All**)

You must select at least one type.

6   For security risk scans, under **Specify the type of security risk scan**, select **Auto-Protect**, **Scheduled and on-demand**, or **All Scans**.

7   Click **OK**.

To exclude a file or folder on Mac clients

1   On the **Exceptions Policy** page, click **Exceptions**.

2   Under **Exceptions**, click **Add > Mac Exceptions > Security Risk Exceptions for File or Folder**.

3   Under **Security Risk File or Folder Exception**, in the **Prefix variable** drop-down box, select a common folder.

Select **[NONE]** to enter the absolute path and file name.

4   In the **File or Folder** text box, type the name of the folder.

If you select a prefix variable, the path should be relative to the prefix. If you select **[NONE]**, type the full path name.

Note: Folder paths must be denoted by using a forward slash.

---

5   Click **OK**.

See "Creating exceptions for Symantec Endpoint Protection" on page 530.

Excluding known risks from virus and spyware scans

The security risks that the client software detects appear in the **Known Security Risk Exceptions** dialog box.

The known security risks list includes information about the severity of the risk.

See "Creating exceptions for Symantec Endpoint Protection" on page 530.

To exclude known risks from virus and spyware scans

1 On the **Exceptions Policy** page, click **Exceptions**.

2 Under **Exceptions**, click **Add > Windows Exceptions > Known Risks**.

3 In the **Add Known Security Risk Exceptions** dialog box, select one or more security risks that you want to exclude from virus and spyware scans.

4 Check **Log when the security risk is detected** if you want to log the detection.

If you do not check this option, the client ignores the risk when it detects the selected risks. The client therefore does not log the detection.

5 Click **OK**.

6 If you are finished with the configuration for this policy, click **OK**.

Excluding file extensions from virus and spyware scans

You can add multiple file extensions to an exception. After you create the exception, you cannot create another extensions exception for the same policy. You must edit the existing exception.

You can add only one extension at a time. If you enter multiple extension names in the **Add** text box, the policy treats the entry as a single extension name.

See "Creating exceptions for Symantec Endpoint Protection" on page 530.

To exclude file extensions from virus and spyware scans

1 On the **Exceptions Policy** page, click **Exceptions**.

2 Under **Exceptions**, click **Add > Windows Exceptions > Extensions**.

3 In the text box, type the extension that you want to exclude, and then click **Add**.

4 Add any other extensions to the exception.

5 Click **OK**.

Monitoring an application to create an exception for the application

When Symantec Endpoint Protection learns a monitored application, the application appears in the **Application Exception** dialog. You can create an exception action for the application in the Exceptions policy. The application also appears in the relevant log, and you can create an exception from the log.

If you disable application learning, the Application to Monitor exception forces application learning for the specified application.

See "Monitoring the applications and services that run on client computers" on page 311.

See "Creating exceptions for Symantec Endpoint Protection" on page 530.

See "Specifying how Symantec Endpoint Protection handles monitored applications" on page 537.

See "Creating exceptions from log events in Symantec Endpoint Protection Manager" on page 541.

To monitor an application to create an exception for the application

1   On the **Exceptions Policy** page, click **Exceptions**.

2   Click **Add > Windows Exceptions > Application to Monitor**.

3   In the dialog box, type the application name.

    For example, you might type the name of an executable file as follows:

    foo.exe

4   Click **Add**.

5   If you are finished with the configuration for this policy, click **OK**.

Specifying how Symantec Endpoint Protection handles monitored applications

You can monitor a particular application so that you can create an exception for how Symantec Endpoint Protection handles the application. After Symantec Endpoint Protection learns the application and the management console receives the event, the application appears in the application list in the **Application Exception** dialog. The application list appears empty if the client computers in your network have not yet learned any applications.

The applications list includes the applications that you monitor as well as the files that your users download. Symantec Endpoint Protection applies the action when either Symantec Endpoint Protection detects the application or the application runs.

The applications also appear in the list for **DNS and Host File Change Exception**.

See "Monitoring an application to create an exception for the application" on page 537.

See "Creating exceptions for Symantec Endpoint Protection" on page 530.

See "Monitoring the applications and services that run on client computers" on page 311.

See "Creating an exception for an application that makes a DNS or host file change" on page 540.

To specify how Symantec Endpoint Protection handles monitored applications

1 On the **Exceptions Policy** page, click **Exceptions**.

2 Click **Add > Windows Exceptions > Application**.

3 In the **View** drop-down list, select **All**, **Watched Applications**, or **User-allowed Applications**.

4 Select the applications for which you want to create an exception.

5 In the **Action** drop-down box, select **Ignore**, **Log only**, **Quarantine**, **Terminate**, or **Remove**.

   The **Ignore** and **Log only** actions apply when scans detect the application. The **Terminate**, **Quarantine**, and **Remove** actions apply when the application launches.

6 Click **OK**.

Excluding a trusted Web domain from scans

You can exclude a Web domain from virus and spyware scans and SONAR.

You can specify only one Web domain at a time. You must specify an HTTP or HTTPS URL or an IP address when you specify a trusted Web domain exception. FTP URLs are not supported in the exceptions configuration. You must specify an IP address for an FTP location. You cannot use a port number.

Note: If Download Insight or Auto-Protect is disabled, trusted Web domain exceptions are disabled as well.

See "Creating exceptions for Symantec Endpoint Protection" on page 530.

To exclude a trusted Web domain from scans

1   On the **Exceptions Policy** page, click **Add > Windows Exceptions > Trusted Web Domain**.

2   In the **Add Trusted Web Domain Exception** dialog box, enter the HTTP or HTTPS Web site or IP address that you want to exclude.

3   Click **OK**.

4   Repeat the procedure to add more Web domain exceptions.

Creating a Tamper Protection exception

You can create file exceptions for Tamper Protection. You might want to create a Tamper Protection exception if Tamper Protection interferes with a known safe application on your client computers. For example, Tamper Protection might block an assistive technology application, such as a screen reader.

You need to know the name of the file that is associated with the assistive technology application. Then you can create an exception to allow the application to run.

Note: Tamper Protection does not support folder exceptions.

See "Creating exceptions for Symantec Endpoint Protection" on page 530.

To create an exception for Tamper Protection

1   On the **Exceptions Policy** page, click **Exceptions**.

2   Click **Add > Windows Exceptions > Tamper Protection Exception**.

3   In the **Add Tamper Protection Exception** dialog box, in the **Prefix variable** drop-down box, select a common folder.

When you select a prefix, the exception can be used on different Windows operating systems.

Select **[NONE]** if you want to enter the absolute path and file name.

4   In the **File** text box, type the name of the file.

If you selected a prefix, the path should be relative to the prefix. If you selected **[NONE]** for the prefix, type the full path name.

You must specify a file name. Tamper Protection does not support folder exceptions. If you enter a folder name, Tamper Protection does not exclude all the files in a folder with that name. It only excludes a file with that specified name.

5   Click **OK**.

Creating an exception for an application that makes a DNS or host file change

You can create an exception for a specific application that makes a DNS or host file change. SONAR might prevent system changes like DNS or host file changes. You might need to make an exception for a VPN application, for example.

You can monitor a particular application so that you can create a DNS or host file change exception. After Symantec Endpoint Protection learns the application and the management console receives the event, the application appears in the application list. The application list appears empty if the client computers in your network have not yet learned any applications.

Use the SONAR settings to control how SONAR detects DNS or host file changes globally.

To create an exception for an application that makes a DNS or host file change

1   On the **Exceptions Policy** page, click **Exceptions**.

2   Click **Add > Windows Exceptions > DNS or Host File Change Exception**.

3   Select the applications for which you want to create an exception.

4   In the **Action** drop-down box, select **Ignore**, **Log only**, **Prompt**, or **Block**.

The actions apply when scans detect the application making a DNS or host file change.

5   Click **OK**.

See "Creating exceptions for Symantec Endpoint Protection" on page 530.

See "Specifying how Symantec Endpoint Protection handles monitored applications" on page 537.

See "Adjusting SONAR settings on your client computers" on page 402.

Restricting the types of exceptions that users can configure on client computers

You can configure restrictions so that users on client computers cannot create exceptions for virus and spyware scans or for SONAR. By default, users are permitted to configure exceptions.

Users on client computers can never create exceptions for Tamper Protection, regardless of the restriction settings.

Users also cannot create file exceptions for application control.

See "Managing exceptions for Symantec Endpoint Protection" on page 528.

To restrict the types of exceptions that users can configure on client computers

1   On the **Exceptions Policy** page, click **Client Restrictions**.

2   Under **Client Restrictions**, uncheck any exception that you do not want users on client computers to configure.

3   If you are finished with the configuration for this policy, click **OK**.

Creating exceptions from log events in Symantec Endpoint Protection Manager

You can create exceptions from log events for virus and spyware scans, SONAR, application control, and Tamper Protection.

Note: You cannot create exceptions from log events for early launch anti-malware detections.

Table 23-4   Exceptions and log types

Exception Type	Log Type
File	Risk log
Folder	Risk log SONAR log
Known risk	Risk log
Extension	Risk log

Table 23-4   Exceptions and log types *(continued)*

Exception Type	Log Type
Application	Risk log
	SONAR log
Trusted Web domain	Risk log
	SONAR log
Tamper Protection	Application Control log
DNS or host file change	SONAR log

See "Monitoring endpoint protection" on page 603.

Symantec Endpoint Protection must have already detected the item for which you want to create an exception. When you use a log event to create an exception, you specify the Exceptions policy that should include the exception.

See "Managing exceptions for Symantec Endpoint Protection" on page 528.

See "Creating exceptions for Symantec Endpoint Protection" on page 530.

To create exceptions from log events in Symantec Endpoint Protection Manager

1   On the **Monitors** tab, click the **Logs** tab.

2   In the **Log type** drop-down list, select the Risk log, SONAR log, or Application and Device Control log.

3   If you selected Application and Device Control, select **Application Control** from the **Log content** list.

4   Click **View Log**.

5   Next to **Time range**, select the time interval to filter the log.

6   Select the entry or entries for which you want to create an exception.

7   Next to **Action**, select the type of exception that you want to create.

    The exception type that you select must be valid for the item or items that you selected.

8   Click **Apply** or **Start**.

9   In the dialog box, remove any items that you do not want to include in the exception.

10 For security risks, check **Log when the security risk is detected** if you want Symantec Endpoint Protection to log the detection.

11 Select all of the Exceptions policies that should use the exception.

12 Click **OK**.

Configuring updates and updating client computer protection

This chapter includes the following topics:

- Configuring the disk space that is used for LiveUpdate downloads

- About randomization of simultaneous content downloads

- Randomizing content downloads from the default management server or a Group Update Provider

- Randomizing content downloads from a LiveUpdate server

- Configuring client updates to run when client computers are idle

- Configuring client updates to run when definitions are old or the computer has been disconnected

- Setting up an external LiveUpdate server

- Setting up an internal LiveUpdate server

- Using Group Update Providers to distribute content to clients

- Using Intelligent Updater files to update client virus and security risk definitions

- Using third-party distribution tools to update client computers

Managing content updates

Symantec products depend on current information to protect computers from threats with the latest threat protection technology. Client computers and servers need periodic updates to their protection content, such as virus and spyware definitions, intrusion protection system signatures, and product software. LiveUpdate provides these Symantec-signed updates through an Internet connection. The LiveUpdate client verifies them to ensure that the updates come from Symantec and have not been tampered with in any way.

Symantec Endpoint Protection supports the HTTPS, HTTP, and FTP protocols to connect to internal LiveUpdate servers. It supports connections to the Symantec LiveUpdate server over HTTP, with FTP as the backup method. Although HTTPS is not supported for connection to the Symantec LiveUpdate server, the content is digitally signed. The advantage of HTTP is that most clients can connect to the LiveUpdate server over HTTP, and HTTP is typically faster.

Note: The LiveUpdate that Symantec Endpoint Protection uses does not update content in other Symantec products. If you previously used a single instance of LiveUpdate for content updates on multiple products, you should now enable the LiveUpdate scheduler in those other Symantec products.

To configure updates for clients, you use the following policies:

■ LiveUpdate Settings policy

■ LiveUpdate Content policy

The LiveUpdate Settings policy specifies the content servers that client computers contact to check for updates and how often clients check for updates. The LiveUpdate Content policy specifies the content types that your client computers download. You can also configure some of the content types that are downloaded to the management server on the **LiveUpdate** tab of the **Site Properties** dialog box.

If you use a LiveUpdate server, the LiveUpdate Settings policy provides **Advanced Settings** for the following areas:

■ The degree of user control over LiveUpdate
You can let users manually start LiveUpdate from their client computers. This setting is disabled by default. If you enable this setting, users can start LiveUpdate and download the latest content virus definitions, component updates, and product updates. Depending on the size of your user population, you may not want to let users download all content without previous testing. Additionally, conflicts can occur if two LiveUpdate sessions run simultaneously on client computers.
You can also choose to let users change their LiveUpdate schedule and change their proxy settings.

■ Download of product updates
By default, users are not allowed to download product updates from a LiveUpdate server, but you can change this setting.

■ Use of standard HTTP headers
LiveUpdate sometimes uses non-standard headers that a firewall might block. You can use this setting to make Symantec Endpoint Protection Manager require standard HTTP headers from LiveUpdate. This setting applies only to downloads to clients from an external or an internal LiveUpdate server.

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

Table 24-1 describes some of the tasks that you can perform to manage content updates. Since you can use the defaults for updating, all tasks are optional.

Table 24-1 Tasks for managing content updates

Task	Description
Run LiveUpdate after installation	After you install Symantec Endpoint Protection Manager, it is configured to periodically update content automatically. However, you can run LiveUpdate immediately or at any point to download the latest security and product updates. See "Downloading LiveUpdate content manually to Symantec Endpoint Protection Manager" on page 563.
Configure the LiveUpdate download settings for the management server	Configure the management server to receive regular content updates. These content updates can be distributed to client computers. When you configure a site to download LiveUpdate content to Symantec Endpoint Protection Manager, you need to make the following decisions: ■ How often the site checks for LiveUpdate content updates. ■ What content types to download to the site. ■ The languages for update types to download. ■ The LiveUpdate server that serves the content to the site. ■ The number of content revisions to keep and whether to store the client packages unzipped. See "Configuring a site to download content updates" on page 559. See "Configuring the disk space that is used for LiveUpdate downloads" on page 571. See "Configuring the LiveUpdate download schedule for Symantec Endpoint Protection Manager" on page 563. See "Checking LiveUpdate server activity" on page 564.
Set up a connection to allow a proxy server to connect to the Symantec LiveUpdate server	Establish communication between a proxy server and Symantec Endpoint Protection Manager so that it can connect with Symantec subscription services. A proxy server can provide an additional level of protection between your site and an external Symantec LiveUpdate server. See "Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate" on page 564.
Specify proxy settings for client communication to an internal LiveUpdate server	You can specify proxy settings for the clients that connect to an internal LiveUpdate server for updates. The proxy settings are for updates only. They do not apply to other types of external communication that clients use. You configure the proxy for other types of client external communication separately. See "Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server" on page 565.

Task	Description
Decide how client computers get updates	Client computers can automatically download security definitions and other product updates from Symantec Endpoint Protection Manager, but several other content distribution methods are available. For example, you can allow users who travel with portable computers to use an Internet connection to get updates directly from a Symantec LiveUpdate server.
	Some installations that have large numbers of clients may set up single or multiple Group Update Providers to reduce the load on the management server. You can also configure an explicit list of Group Update Providers that clients can use to connect to Group Update Providers that are on subnets other than the client's own subnet.
	Note: Mac clients get updates only from an internal or an external LiveUpdate server.
	See "About the types of content that LiveUpdate can provide" on page 549.
	See "How client computers receive content updates" on page 554.
	See "Configuring the LiveUpdate download schedule for client computers" on page 568.
Configure the amount of control to give users over LiveUpdate	You can decide how much control to give your users over their content updates.
	See "Configuring the amount of control that users have over LiveUpdate" on page 569.
Tune client download parameters	To mitigate the effect of downloads on network bandwidth, you can download content randomly so that not all clients get updates at the same time.
	See "About randomization of simultaneous content downloads" on page 572.
	See "Randomizing content downloads from the default management server or a Group Update Provider" on page 573.
	To mitigate the effect of downloads on client computers' performance, you can have the client computers download content updates when the client computers are idle.
	See "Configuring client updates to run when client computers are idle" on page 574.
Configure an alternate distribution method	Client computers automatically download virus definitions and other content updates from Symantec Endpoint Protection Manager, but there are several alternate distribution methods that you can use.
	See "How client computers receive content updates" on page 554.

About the types of content that LiveUpdate can provide

The types of content that LiveUpdate can provide include virus and spyware definitions, Intrusion Prevention System signatures, and product updates. To control the content types that your client computers download, you use a LiveUpdate Content policy. To control the content types that the default management server downloads to distribute to clients, you configure the properties

settings for the site. If content is selected in a LiveUpdate policy but is not selected in the site properties, that content is not delivered to the clients.

Note: Typically, you should not need to restrict the content that Symantec Endpoint Protection Manager downloads. Be careful to only turn off a type of content if you are certain that you do not need it.

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

Table 24-2 lists the types of content that you can configure in Symantec Endpoint Protection Manager to download to clients.

Table 24-2   The content types that you can configure for download to the clients

Content type	Description
Product updates	Product updates are improvements to the installed client software. These updates are usually created to extend the operating system or hardware compatibility, adjust performance issues, or fix product errors. Product updates are released on an as-needed basis. Clients can receive product updates directly from a LiveUpdate server. Managed clients can also receive product updates from Symantec Endpoint Protection Manager. ■ The **Product Update Settings** parameter in the **Advanced Settings** of a LiveUpdate Settings policy lets you control your client software versions. This choice is not configured in a LiveUpdate Content policy. When this setting is enabled, client software can be updated through LiveUpdate. ■ The Symantec Endpoint Protection Manager downloads client updates by default through LiveUpdate. This setting can be disabled in the site properties for Symantec Endpoint Protection Manager. When an update is downloaded, it appears in the **Client Install Packages** pane. You can then select the package, and use the **Upgrade Clients with Package** feature for your Windows clients. You can use the **Client Deployment Wizard** to update your Mac clients. **Web link and email** creates a package and sends the download URL to the intended email recipients. **Save package** builds and exports an installation package. This package can then be deployed with a third-party tool, or placed in a network location for download and manual installation.
Virus and Spyware definitions	Separate virus definition packages are available for the x86 and the x64 platforms. This content type also includes the Auto-Protect portal list.
SONAR heuristic signatures	Protects against zero-day attack threats.

Table 24-2	The content types that you can configure for download to the clients *(continued)*

Content type	Description
TruScan proactive threat scan commercial application list	Includes the legitimate commercial applications that have generated false positives in the past. These are used for backward compatibility when you manage legacy clients.
Intrusion Prevention signatures	Protects against network threats and supports the intrusion prevention and detection engines.
Submission Control signatures	Controls the flow of submissions to Symantec Security Response.
Reputation Settings	Includes the updates to the reputation data that is used in protection.
Host Integrity content	Includes the templates of predefined requirements that enforce updated patches and security measures on the client computer. LiveUpdate downloads templates for the computers that run Windows operating systems and Mac operating systems. See "Adding a Host Integrity requirement from a template" on page 820. **Note:** This option only appears in the **Site Properties** dialog box when you install Symantec Network Access Control.

Note: You cannot exclude all types of content. For example, the **Extended File Attributes and Signatures** that are used to control root certificate and signer information are always downloaded.

See "Managing content updates" on page 546.

See "How client computers receive content updates" on page 554.

See "Configuring the types of content used to update client computers" on page 567.

Table 24-3 lists the features that need regular updates and the types of content that each feature needs.

Table 24-3   Features and the update content that they need

When you install an unmanaged client	When you update, you need to download these types of content
Virus and Spyware Protection	■ Virus and Spyware Definitions ■ SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures. ■ Symantec Whitelist When you configure a site to download content, this content type is called TruScan proactive threat scan commercial application list. ■ Revocation Data (downloaded by default, not configurable from Symantec Endpoint Protection Manager) ■ Centralized Reputation Settings When you configure content types for download in Site Properties, this content type is called Reputation Settings. ■ Submission Control signatures ■ Auto-Protect portal list
Virus and Spyware Protection > Download Protection	■ Virus and Spyware Definitions ■ SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures. ■ Symantec Whitelist When you configure a site to download content, this content type is called TruScan proactive threat scan commercial application list. ■ Revocation Data (downloaded by default, not configurable from Symantec Endpoint Protection Manager) ■ Centralized Reputation Settings When you configure content types for download in Site Properties, this content type is called Reputation Settings. ■ Intrusion Prevention signatures When you select this option to download, it includes updates to both the Intrusion Prevention signatures and the Intrusion Prevention engines. ■ Submission Control signatures ■ Auto-Protect portal list

Table 24-3   Features and the update content that they need *(continued)*

When you install an unmanaged client	When you update, you need to download these types of content
Virus and Spyware Protection > Outlook Scanner	■ Virus and Spyware Definitions ■ SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures. ■ Symantec Whitelist When you configure a site to download content, this content type is called TruScan proactive threat scan commercial application list. ■ Revocation Data (downloaded by default, not configurable from Symantec Endpoint Protection Manager) ■ Centralized Reputation Settings When you configure content types for download in Site Properties, this content type is called Reputation Settings. ■ Submission Control signatures ■ Auto-Protect Portal List
Virus and Spyware Protection > Notes Scanner	■ Virus and Spyware Definitions ■ SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures. ■ Symantec Whitelist When you configure a site to download content, this content type is called TruScan proactive threat scan commercial application list. ■ Revocation Data (downloaded by default, not configurable from Symantec Endpoint Protection Manager) ■ Centralized Reputation Settings When you configure content types for download in Site Properties, this content type is called Reputation Settings. ■ Submission Control signatures ■ Auto-Protect Portal List
Proactive Threat Protection > SONAR	SONAR Definitions Submission Control signatures When you configure content types for download in Symantec Endpoint Protection Manager, these are called SONAR heuristic signatures.
Proactive Threat Protection > Application and Device Control	Submission Control signatures

Table 24-3	Features and the update content that they need *(continued)*
When you install an unmanaged client	**When you update, you need to download these types of content**
Network Threat Protection > Intrusion Prevention	Intrusion Prevention signatures Submission Control signatures **Note:** When you select this option to download, it includes updates to both the intrusion prevention signatures and the Intrusion Prevention engines.
Network Threat Protection > Firewall	Submission Control signatures
Network Access Control	Host Integrity content Submission Control signatures

Note: You cannot configure **Extended File Attributes and Signatures** and **Submission control signatures**. They are always installed.

How client computers receive content updates

Client computers can use LiveUpdate to download security definitions and other product updates automatically, but you can also use several other content distribution methods to update clients.

The LiveUpdate server schedule settings are defined in the **Site Properties** on the **Admin** page. The LiveUpdate client schedule settings are defined in the LiveUpdate Settings policy.

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

The content distribution methods that you use depend on the following factors:

- How you set up your network.

- How many client computers you manage.
  For example, if you have a very large number of clients, you can use Group Update Providers to ease the load on your management servers. You can even

set up internal LiveUpdate servers using LiveUpdate Administrator, if
necessary.

■ Whether you manage Windows and Mac client computers.
For example, Mac client computers get updates only from an internal or an
external LiveUpdate server. Only Windows client computers can get updates
from the management server or Group Update Provider.

■ Whether client computers regularly connect to your network.
For example, some users may travel with portable computers that connect
intermittently or not at all to your network. In this case, you can allow the
client computers to get updates directly from a Symantec LiveUpdate server
using the Internet.

See "Managing content updates" on page 546.

Table 24-4   Content distribution methods and when to use them

Method	Description	When to use it
Symantec Endpoint Protection Manager to client computers (Default)	The default management server can update the client computers that it manages. You might have multiple management servers in your Symantec Endpoint Protection Manager network. The site that includes the management servers receives LiveUpdate content.	**Note:** Only Windows client computers can get updates from the management server. Mac client computers must currently get their updates from a Symantec LiveUpdate server or manually. See "Using Intelligent Updater files to update client virus and security risk definitions" on page 593. This method is configured by default after management server installation. You can also combine this method with a Group Update Provider.
Group Update Provider to client computers	A Group Update Provider is a client computer that receives updates from a management server. It then forwards the updates to the other client computers in the group. A Group Update Provider can update multiple groups. Note that Group Update Providers distribute all types of LiveUpdate content except client software updates. Group Update Providers also cannot be used to update policies.	Setting up a Group Update Provider is easier than setting up an internal LiveUpdate server. Group Update Providers are less resource-intensive and so reduce the load on the management servers. This method is particularly useful for groups at remote locations with minimal bandwidth. See "Using Group Update Providers to distribute content to clients " on page 580.

| | Table 24-4 | Content distribution methods and when to use them *(continued)* |

Method	Description	When to use it
Internal LiveUpdate server to client computers	Client computers can download updates directly from an internal LiveUpdate server that receives its updates from a Symantec LiveUpdate server.	You can use an internal LiveUpdate server in very large networks to reduce the load on the Symantec Endpoint Protection Manager. You should first consider whether Group Update Providers would meet your organization's needs. Group Update Providers are easier to set up and also reduce the load on the management servers.
	You use the LiveUpdate Administrator utility to download the definitions updates down from a Symantec LiveUpdate server. The utility places the packages on a Web server, an FTP site, or a location that is designated with a UNC path. You configure your management servers and client computers to download their definitions updates from this location.	Use an internal LiveUpdate server if you have Mac clients and you don't want them to connect to a Symantec LiveUpdate server over the Internet.
	If necessary, you can set up several internal LiveUpdate servers and distribute the list to client computers.	An internal LiveUpdate server is also useful if your organization runs multiple Symantec products that also use LiveUpdate to update client computers.
	For more information about setting up an internal LiveUpdate server, see the *LiveUpdate Administrator User's Guide.*	You typically use an internal LiveUpdate server in large networks of more than 10,000 clients.
	The guide is available on the Tools product disc and on the Symantec Support Web site.	**Note:** You should not install Symantec Endpoint Protection Manager and an internal LiveUpdate server on the same physical hardware or virtual machine. Installation on the same computer can result in significant server performance problems.
		For more information see the knowledge base article: LiveUpdate Administrator 2.x and Symantec Endpoint Protection Manager on the same computer.
		See "Setting up an internal LiveUpdate server" on page 577.

Table 24-4   Content distribution methods and when to use them *(continued)*

Method	Description	When to use it
Symantec LiveUpdate server to client computers over the Internet	Client computers can receive updates directly from a Symantec LiveUpdate server. **Note:** Mac client computers must use this method.	Use an external Symantec LiveUpdate server for the client computers that are not always connected to the corporate network. Symantec Endpoint Protection Manager and scheduled updates are enabled by default, as are the options to only run scheduled updates when connection to Symantec Endpoint Protection Manager is lost and the virus and spyware definitions are older than a certain age. With the default settings, clients always get updates from Symantec Endpoint Protection Manager except when Symantec Endpoint Protection Manager is nonresponsive for a long period of time. **Note:** Do not configure large numbers of managed, networked clients to pull updates from an external Symantec LiveUpdate server. This configuration consumes unnecessary amounts of Internet bandwidth. See "Setting up an external LiveUpdate server" on page 576.
Third-party tool distribution	Third-party tools like Microsoft SMS let you distribute specific update files to clients.	Use this method when you want to test update files before you distribute them. Also, use this method if you have a third-party tool distribution infrastructure, and want to leverage the infrastructure. See "Distributing the content using third-party distribution tools" on page 598.

Method	Description	When to use it
Intelligent Updater	Intelligent Updater files contain the virus and security risk content that you can use to manually update clients. You can download the Intelligent Updater self-extracting files from the Symantec Web site.	You can use Intelligent Updater files if you do not want to use Symantec LiveUpdate or if LiveUpdate is not available. See "Using Intelligent Updater files to update client virus and security risk definitions" on page 593. To update other kinds of content, you must set up and configure a management server to download and to stage the update files. See "Using third-party distribution tools to update client computers" on page 594.

Figure 24-1 shows an example distribution architecture for smaller networks.

Figure 24-1 Example distribution architecture for smaller networks
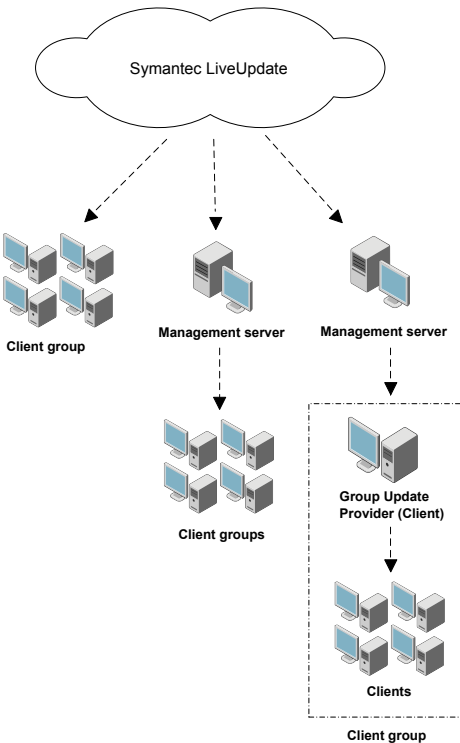
shows an example distribution architecture for larger networks.

Figure 24-2   Example distribution architecture for larger networks
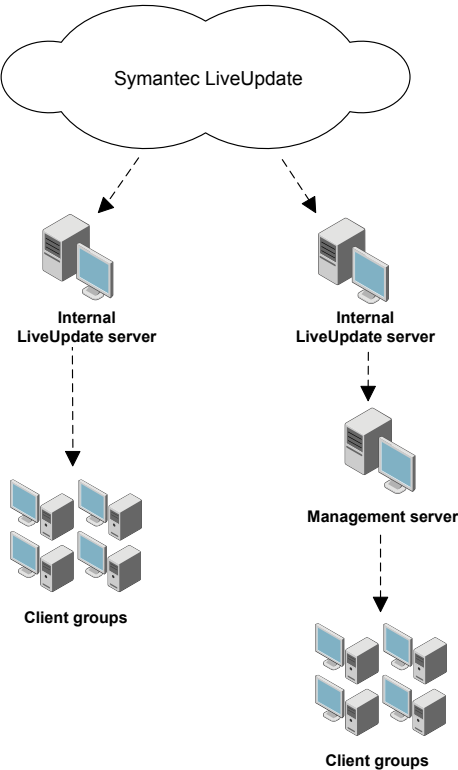
Configuring a site to download content updates

When you configure a site to download LiveUpdate content, you have to make a number of decisions.

Table 24-5   Decisions about content downloads

Decision	Description
How often should my site check for LiveUpdate content updates?	The default schedule of having Symantec Endpoint Protection Manager run LiveUpdate every four hours is a best practice.

| Table 24-5 | Decisions about content downloads *(continued)* |

Decision	Description
What content types should I download to the site?	Make sure that the site downloads all content updates that are specified in your client LiveUpdate Content policies. See "About the types of content that LiveUpdate can provide" on page 549. See "Configuring the types of content used to update client computers" on page 567.
What languages should be downloaded for product updates?	This setting on the **Site Properties** dialog box applies only to product updates; the content updates are suitable for all languages.
What LiveUpdate server should serve the content to the site?	You can specify either an external Symantec LiveUpdate server (recommended), or one or more internal LiveUpdate servers that have previously been installed and configured. See "Setting up an external LiveUpdate server" on page 576. You should not install Symantec Endpoint Protection Manager and an internal LiveUpdate server on the same physical hardware or virtual machine. Installation on the same computer can result in significant server performance problems. If you decide to use one or more internal LiveUpdate servers, you may want to add the Symantec public LiveUpdate server as the last entry. If your clients cannot reach any server on the list, then they are still able to update from the Symantec LiveUpdate server. **Note:** If you use LiveUpdate Administrator version 1.x to manage your internal LiveUpdate server, you need to make a change if you applied custom Response packages. LiveUpdate clients that use the current release cannot authenticate custom Response packages. You should remove any custom packages from the central LiveUpdate server. See "Setting up an internal LiveUpdate server" on page 577.

Table 24-5   Decisions about content downloads *(continued)*

Decision	Description
How many content revisions should the site store and should the client packages be stored unzipped?	One good reason to store multiple revisions of a single content type is to provide the ability to create and distribute deltas to clients. When Symantec Endpoint Protection Manager and the client have a content revision in common, Symantec Endpoint Protection Manager can use it as a base for a delta to send to clients. Clients can apply that delta to the same base locally to get the latest content. Deltas are typically much smaller than full packages, which results in major bandwidth savings.

You might also store content revisions because you might want to test the latest content before you roll it out to all your clients. You might want to keep earlier versions of the content so that you can roll back if necessary.

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

See "Configuring the disk space that is used for LiveUpdate downloads" on page 571.

See "Configuring the content revisions that clients use" on page 570. |

To configure a site to download updates

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

2   Under **Servers**, right-click **Local Site**, and then click **Edit Site Properties**.

3   On the **LiveUpdate** tab, in the **Download Schedule** group box, click **Edit Schedule**, set the options for how often the server should check for updates.

4   Click **OK**.

5   Under **Content Types to Download**, inspect the list of update types that are downloaded.

6   To add or delete an update type, click **Change Selection**, modify the list, and then click **OK**.

The list should match the list of content types that you include in the LiveUpdate Content policy for your client computers.

7   Under **Languages to Download**, inspect the list of languages of the update types that are downloaded.

8   To add or delete a language, click **Change Selection**, modify the list, and then click **OK**.

9   Under **Platforms to Download**, click **Change Platforms** and then inspect the platforms list. Uncheck the platforms that you do not want to download content to.

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

- ■ To use the existing LiveUpdate Source server, click **OK**.

- ■ To use an internal LiveUpdate server, click **Use a specified internal LiveUpdate server** and then click **Add**.

11 If you selected **Use a specified internal LiveUpdate server**, in the **Add LiveUpdate Server** dialog box, complete the boxes with the information that identifies the LiveUpdate server, and then click **OK**.

You can add more than one server for failover purposes. If one server goes offline, the other server provides support. You can also add the Symantec public LiveUpdate server as the last server in the list. If you add the public server, use **http://liveupdate.symantecliveupdate.com** as the URL.

Note: If you use a UNC server, then LiveUpdate requires that you use the domain or workgroup as part of the user name.

If the computer is in a domain, use the format *domain_name\user_name*.

If the computer is in a workgroup, use the format *computer_name\user_name*.

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

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

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

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

Note: Disabling this option also disables the ability of Symantec Endpoint Protection to construct deltas between content revisions and may adversely affect network performance for updates.

15 Click **OK**.

See "Managing content updates" on page 546.

Configuring the LiveUpdate download schedule for Symantec Endpoint Protection Manager

You can adjust the schedule that Symantec Endpoint Protection Manager uses to download content updates from LiveUpdate to the management server. For example, you can change the default server schedule frequency from hourly to daily to save bandwidth.

To configure the schedule for LiveUpdate downloads to Symantec Endpoint Protection Manager

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

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

3   Select the site, then under **Tasks**, click **Edit Site Properties**.

4   In the **Server Properties** dialog box, on the **LiveUpdate** tab, click **Edit Schedule**.

5   Change the frequency and any other settings that you want to change.

6   Click **OK**.

See "Managing content updates" on page 546.

Downloading LiveUpdate content manually to Symantec Endpoint Protection Manager

You do not have to wait for your scheduled LiveUpdate downloads. You can manually download content updates to Symantec Endpoint Protection Manager. You can use either of the following procedures.

To manually download content updates to Symantec Endpoint Protection Manager

1   From the **Home Page**, select **Common Tasks** and then select **Run LiveUpdate**.

2   Click **Download**.

To manually download content updates to Symantec Endpoint Protection Manager

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

2   On the **Admin** page, click **Servers**, and then select the site.

3 Click **Download LiveUpdate content**.

4 In the **Download LiveUpdate Content** dialog box, review the properties, and then click **Download**.

If you need to change any of the properties, click **Cancel** and change the properties first.

See "Configuring a site to download content updates" on page 559.

See "Managing content updates" on page 546.

Checking LiveUpdate server activity

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

To check LiveUpdate server activity

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

2 On the **Admin** page, under **Tasks**, click **Servers** and select the site.

3 Click **Show the LiveUpdate Status**.

4 Click **Close**.

See "Managing content updates" on page 546.

Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate

If you want Symantec Endpoint Protection Manager to go through a proxy server to connect to the Internet, you must configure Symantec Endpoint Protection Manager to connect to the proxy server. A proxy server can add a layer of security because only the proxy server is connected directly to the Internet.

To configure Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate

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

2 Under **Servers**, select the management server to which you want to connect a proxy server.

3 Under **Tasks**, click **Edit the server properties**.

4   On the **Proxy Server** tab, under either **HTTP Proxy Settings** or **FTP Proxy Settings**, for **Proxy usage**, select **Use custom proxy settings**.

5   Type in the proxy settings.

     For more information on these settings, click **Help**.

6   Click **OK**.

See "Managing content updates" on page 546.

Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server

You can specify a proxy server that your clients use to communicate with an internal LiveUpdate server. The proxy settings do not affect any settings for Group Update Providers.

See "Managing content updates" on page 546.

Note: You configure proxy settings for other client communications separately.

To specify a proxy server that clients on Windows computers use to communicate to Symantec LiveUpdate or an internal LiveUpdate server

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

2   Under **Policies**, click **LiveUpdate**, and then click the **LiveUpdate Settings** tab.

3   Right-click the policy that you want and then select **Edit**.

4   Under **Windows Settings**, click **Server Settings**.

5   Under **LiveUpdate Proxy Configuration**, click **Configure Proxy Options**.

6   On the **HTTP or HTTPS** tab or the **FTP** tab, select the desired options.

     See the online Help for more information about the options.

7   Click **OK** in the dialog box.

8   Click **OK**.

To specify a proxy server that clients on Mac computers use to communicate to Symantec LiveUpdate or an internal LiveUpdate server

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

2   Under **Location-independent Policies and Settings**, under **Settings**, click **External Communication Settings**.

3   On the **Proxy Server (Mac)** tab, select the desired options.

     See the online Help for more information about the options.

4   Click **OK**.

Enabling and disabling LiveUpdate scheduling for client computers

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

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

To enable LiveUpdate scheduling for client computers

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

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

3   On the **LiveUpdate Settings** tab, right-click the policy that you want, and then click **Edit**.

4   Under **Windows Settings**, click **Schedule**.

5   Check **Enable LiveUpdate Scheduling**.

6   Specify the frequency and the retry window.

7   Click **OK**.

To disable LiveUpdate scheduling for client computers

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

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

3   On the **LiveUpdate Settings** tab, right-click the policy that you want, and then click **Edit**.

4   Under **Windows Settings**, click **Schedule**.

5   Uncheck **Enable LiveUpdate Scheduling**.

6   Click **OK**.

See "Managing content updates" on page 546.

Configuring the types of content used to update client computers

The LiveUpdate Content policy specifies the content types that clients are permitted to check for and install. Rolling back content to an old revision can be useful in troubleshooting situations

---

Note: Use this feature very carefully. Unchecking a content type means that the feature is not kept up-to-date on the client. This can potentially put your clients at greater risk.

To configure the update content for client computers

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

2   Under **Policies**, click **LiveUpdate**, and then click the **LiveUpdate Content** tab.

3   Right-click the content policy that you want, and then click **Edit**.

4   Under **Windows Settings**, click **Security Definitions**.

5   Check the types of content updates that you want clients to download and install, and uncheck the types that you don't want.

Note: If you have Mac clients, they can install only updates to virus and spyware definitions. This option, under **Mac Settings**, **Security Definitions**, is enabled by default.

---

6   Optionally, for each update, you can use the latest available content, or select a specific revision from a list of available versions.

7   Click **OK**.

    If you have not already assigned this policy to groups and locations, then you must assign the policy to have it take effect.

See "Configuring a site to download content updates" on page 559.

See "Managing content updates" on page 546.

See "Configuring the content revisions that clients use" on page 570.

Configuring the LiveUpdate download schedule for client computers

The LiveUpdate client schedule settings are defined in the LiveUpdate Settings policy.

To save bandwidth, Symantec Endpoint Protection clients can be configured to only run scheduled LiveUpdates from the Symantec LiveUpdate server if one of the following conditions is met:

- Virus and spyware definitions on a client computer are more than two days old.
- A client computer is disconnected from Symantec Endpoint Protection Manager for more than eight hours.

If you check both options, then a client computer's scheduled LiveUpdate from Symantec runs only if it meets both of the criteria.

To configure the schedule for LiveUpdate downloads to Windows client computers

1   Click **Policies** and then click **LiveUpdate**.

2   On the **LiveUpdate Settings** tab, right-click the policy that you want, and then click **Edit**.

3   Under **Windows Settings**, click **Schedule**.

4   Check **Enable LiveUpdate Scheduling**.

5   Specify the frequency.

    If you select **Daily**, also set the time of day to run. If you select **Weekly**, also set the time of day to run and the day of the week to run.

6   If you select any frequency other than **Continuously**, specify the **Retry Window**.

    The **Retry Window** is the number of hours or days that the client computer tries to run LiveUpdate if the scheduled LiveUpdate fails for some reason.

7   Set the additional options, if desired.

8   Click **OK**.

See

To configure the schedule for LiveUpdate downloads to Mac client computers

1   Click **Policies** and then click **LiveUpdate**.

2   On the **LiveUpdate Settings Policy** tab, right-click the policy that you want, and then click **Edit**.

3 Under **Mac Settings**, click **Schedule**.

4 Specify the frequency.

If you select **Daily**, also set the time of day to run. If you select **Weekly**, also set the time of day to run and the day of the week to run.

5 Click **OK** when finished.

See

Configuring the amount of control that users have over LiveUpdate

You may want to allow users who travel to use an Internet connection to get updates directly from a Symantec LiveUpdate server. You can also allow users to modify the LiveUpdate schedule you set up for content downloads.

Note: If an unmanaged client has a LiveUpdate Settings policy assigned to it when an install package is created, the policy settings always take precedence over a user's changes once the user restarts the computer. To install an unmanaged client that retains a user's changes to LiveUpdate settings after the computer is restarted, install the client from the product disc. Do not use a client install package that has been exported from the Symantec Endpoint Protection Manager.

To configure the amount of control that users have over LiveUpdate

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

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

3 On the **LiveUpdate Settings** tab, right-click the policy that you want, and then click **Edit**.

4 Under **Windows Settings**, click **Advanced Settings**.

5 Under **User Settings** pane, check **Allow the user to manually launch LiveUpdate**.

6 Optionally, check **Allow the user to modify the LiveUpdate schedule**.

7 Optionally, under **Product Update Settings**, check **Download Symantec Endpoint Protection product updates using a LiveUpdate server**. Enable this option only if you do not need to keep strict control of the client software revisions that your clients use.

See

See "Configuring the LiveUpdate download schedule for client computers"
on page 568.

Configuring the content revisions that clients use

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

Note: If you want to keep strict control of the client software revisions that your
clients use, do not enable them to download product updates.

See "Configuring the amount of control that users have over LiveUpdate"
on page 569.

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

To configure clients use a specific content version

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

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

3   Click the **LiveUpdate Content** tab.

4   Right-click the LiveUpdate Content policy that you want and then click **Edit**.

5   Under **Windows Settings**, click **Security Definitions**.

6   Under the type of content that you want to roll back, click **Select a revision**.

7   Click **Edit** and select the revision that you want to roll back to from the
    Revision drop-down list.

8   Click **OK**.

See "Managing content updates" on page 546.

Configuring the disk space that is used for LiveUpdate downloads

If you select 500 or fewer clients during the Symantec Endpoint Protection Manager installation, then by default Symantec Endpoint Protection Manager stores three LiveUpdate content revisions for each content type. If you select 500 to 1,000 clients, Symantec Endpoint Protection Manager stores 10 revisions by default. If you select more than 1,000 clients, then Symantec Endpoint Protection Manager stores 30 revisions by default. For example, if you select 500 or fewer clients, the Symantec Endpoint Protection Manager stores three revisions.

To reduce disk space and database size, you can reduce the number of content revisions that are kept on the server. You should be aware, however, that reducing the number of content revisions also affects a server's ability to make deltas between content updates. A delta is an update that contains only the incremental changes since the last full content revision. Delta files are typically much smaller than full update files.

The more content revisions that you keep, the greater the ability of the server to create deltas between content revisions. The number of content revisions that you keep is particularly important if you have some client computers that are offline for days at a time. Symantec typically releases 3 to 4 virus and spyware content revisions per day. Keeping at least 10 revisions ensures that the computers that disconnected on a Friday can use a delta to update on Monday morning. Delta updates take less time and bandwidth than downloading a full content revision.

To configure the disk space used for LiveUpdate downloads

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

2   Click **Servers** and select the site that you want to configure.

3   Under **Tasks**, click **Edit Site Properties**, and then click **LiveUpdate**.

4   Under **Disk Space Management for Downloads**, type the number of content downloads that you want to store.

5   If you want to reduce the amount of disk space used, uncheck the **Store client packages unzipped to provide better network performance for upgrades** option.

Note: Disabling this option also disables the ability of Symantec Endpoint Protection Manager to construct deltas between content revisions and may adversely affect network performance for updates.

---

6   Click **OK**.

About randomization of simultaneous content downloads

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

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

In some cases, however, you might want to increase the randomization window value. For example, you might run the Symantec Endpoint Protection client on multiple virtual machines on the same physical computer that runs the management server. The higher randomization value improves the performance of the server but delays content updates to the virtual machines.

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

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

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

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

See "Setting up an internal LiveUpdate server" on page 577.

Randomizing content downloads from the default management server or a Group Update Provider

Your default management server or Group Update Providers might experience reduced performance when multiple client computers attempt to download content from them simultaneously. You can set a randomization window in the communication settings for the group to which the client computers belong. Each client computer attempts to download content at a random time that occurs within that window.

Note: The communication settings do not control the randomization settings for the client computers that download content from a LiveUpdate server. You can change the randomization settings for those computers in the LiveUpdate Settings policy.

See "Randomizing content downloads from a LiveUpdate server" on page 573.

To randomize content downloads from the default management server or a Group Update Provider

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

2   Under **Clients**, click the group that you want.

3   On the **Policies** tab, under **Location-independent Policies and Settings**, under **Settings**, click **Communication Settings**.

4   In the **Communication Settings** dialog box, under **Download Randomization**, check **Enable randomization**.

5   Optionally, change the randomization window duration.

6   Click **OK**.

See "About randomization of simultaneous content downloads" on page 572.

See "Setting up an internal LiveUpdate server" on page 577.

Randomizing content downloads from a LiveUpdate server

Your network might experience traffic congestion when multiple client computers attempt to download content from a LiveUpdate server. You can configure the

update schedule to include a randomization window. Each client computer attempts to download content at a random time that occurs within that window.

Note: The schedule settings in the LiveUpdate Settings policy do not control randomization for the client computers that download content from the default management server or from a Group Update provider. You can change the randomization settings for those computers in the **Communication Settings** dialog box for the group to which they belong.

See "Randomizing content downloads from the default management server or a Group Update Provider" on page 573.

To randomize client content downloads from a LiveUpdate server

1   Click **Policies**.

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

3   On the **LiveUpdate Settings** tab, right-click the policy that you want to edit, and then click **Edit**.

4   Under **Windows Settings**, click **Schedule**.

5   Under **Download Randomization Options**, check **Randomize the start time to be + or - (in hours)**.

Note: This setting is in days, if you select **Weekly** updates.

6   Optionally, change the duration for the randomized start time.

7   Click **OK**.

See "About randomization of simultaneous content downloads" on page 572.

See "Setting up an internal LiveUpdate server" on page 577.

Configuring client updates to run when client computers are idle

To ease client computer performance issues, you can configure content downloads to run when client computers are idle. This setting is on by default. Several criteria, such as user, CPU, and disc actions, are used to determine when the computer is idle.

If **Idle Detection** is enabled, once an update is due, the following conditions can delay the session:

- The user is not idle.

- The computer is on battery power.

- The CPU is busy.

- The disk I/O is busy.

- No network connection is present.

After one hour, the blocking set is reduced to CPU busy, Disk I/O busy, or no network connection exists. Once the scheduled update is overdue for two hours, as long as a network connection exists, the scheduled LiveUpdate runs regardless of idle status.

To configure client updates to run when client computers are idle

1   Click **Policies**.

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

3   On the **LiveUpdate Settings** tab, right-click the policy that you want to edit, and then click **Edit**.

4   Under **Windows Settings**, click **Schedule**.

5   Check **Delay scheduled LiveUpdate until the computer is idle. Overdue sessions will run unconditionally**.

6   Click **OK**.

See "Configuring the LiveUpdate download schedule for client computers" on page 568.

See "Configuring client updates to run when definitions are old or the computer has been disconnected" on page 575.

Configuring client updates to run when definitions are old or the computer has been disconnected

You can ensure that clients update when definitions are old or the computer has been disconnected from the network for a specified amount of time.

Note: If you check both available options, the client computer must meet both conditions.

To configure client updates when definitions are old or the computers is disconnected from the manager

1   Click **Policies**.

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

3   On the **LiveUpdate Settings** tab, right-click the policy that you want to edit, and then click **Edit**.

4   Under **Windows Settings**, click **Schedule**.

5   Check **LiveUpdate runs only if Virus and Spyware definitions are older than:** and then set the number of hours or days.

6   Check **LiveUpdate runs only if the client is disconnected from Symantec Endpoint Protection for more than:** and then set the number of minutes or hours.

7   Click **OK**.

See "Configuring the LiveUpdate download schedule for client computers" on page 568.

See "Configuring client updates to run when client computers are idle" on page 574.

Setting up an external LiveUpdate server

Most organizations should probably use the default management server to update clients, but you can use a Symantec LiveUpdate server instead.

Note: Mac client computers cannot get updates from the default management server.

To set up an external LiveUpdate server for Windows clients

1   Click **Policies**.

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

3   On the **LiveUpdate Settings** tab, right-click the policy that you want and then click **Edit**.

4   Under **Windows Settings**, click **Server Settings**.

5   Click **Use the default Symantec LiveUpdate server**.

6   Click **OK**.

To set up an external LiveUpdate server for Mac clients

1   Click **Policies**.

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

3   On the **LiveUpdate Settings** tab, right-click the policy that you want and then click **Edit**.

4   Under **Mac Settings**, click **Server Settings**.

5   Click **Use the default Symantec LiveUpdate server**.

6   If your internal LiveUpdate server uses FTP, click **Advanced Server Settings**.

7   Click the FTP mode that the server uses, either **Active** or **Passive**.

8   Click **OK**.

See "Managing content updates" on page 546.

Setting up an internal LiveUpdate server

By default, client gets their updates from the management server through Symantec Endpoint Protection Manager. Most organizations should use the default management server for client updates. If you select the default management server and your environment contains Mac and Windows computers, Mac clients get their updates from the default LiveUpdate server. Organizations that have a lot of clients may want to use Group Update Providers (GUPs). GUPs reduce the load on the management server and are easier to set up than an internal LiveUpdate server.

See "Using Group Update Providers to distribute content to clients " on page 580.

If you don't want to use the default management server or Group Update Providers for client updates, you can:

■   Set up an internal LiveUpdate server.

■   Use a Symantec LiveUpdate server that is external to your network.

To use an internal LiveUpdate server, you must perform the following tasks:

■   Install the internal LiveUpdate server.
    If you provide updates to clients from a LiveUpdate Administrator 1.x server, you must go to **Advanced Server Settings** in the LiveUpdate Settings policy and enable support. You must check the checkbox to enabled support for LiveUpdate Administrator Utility 1.x. Support for LiveUpdate Administrator 2.x and later is always enabled.
    See "Setting up an internal LiveUpdate server" on page 577.

For more information about using an internal LiveUpdate server, refer to the
LiveUpdate Administrator's Guide.

Note: If you use LiveUpdate Administrator version 1.x to manage your internal
LiveUpdate server, you must make a change if you have custom Response
packages applied. LiveUpdate clients that use the current release cannot
authenticate custom Response packages. You should remove any custom
packages from the central LiveUpdate server.

■ Use the LiveUpdate Settings policy to configure your clients to use that internal
LiveUpdate server.

To configure Windows clients to use an internal LiveUpdate server

1 Under **Policies**, click **LiveUpdate**.

2 On the **LiveUpdate Settings** tab, right-click the policy that you want and then
   click **Edit**.

3 Under **Windows Settings**, click **Server Settings**.

4 In the **Server Settings** pane, check **Use a LiveUpdate server**.

5 Click **Use a specified internal LiveUpdate server**, and then click **Add**.

6 In the **Add LiveUpdate Server** dialog box, type the information that you need
   to identify and communicate with the server that you want to use.

   For example, for the URL:

   ■ If you use the FTP method (recommended), type the FTP address for the
     server. For example: ftp://myliveupdateserver.com

   ■ If you use the HTTP method, type the URL for the server. For example:
     http://myliveupdateserver.com or 2.168.133.11/Export/Home/LUDepot

   ■ If you use the LAN method, type the server UNC path name. For example,
     \\Myserver\LUDepot

7 If required, type in a user name and password for the server.

Note: If you use a UNC server, then LiveUpdate requires that you use the
domain or workgroup in addition to the user name. If the computer is part
of a domain, use the format *domain_name\user_name*

If the computer is part of a workgroup, use the format
computer_name\user_name.

---

8 Under **LiveUpdate Policy**, click **Schedule** to set up a schedule for updates through LiveUpdate.

See "Configuring the LiveUpdate download schedule for client computers" on page 568.

9 Click **OK**.

10 Click **Advanced Settings**.

Decide whether to keep or change the default user settings, product update settings, and non-standard header settings. Generally, you do not want users to modify update settings. You may, however, want to let users manually launch a LiveUpdate session if you do not support hundreds or thousands of clients.

See "Configuring the amount of control that users have over LiveUpdate" on page 569.

11 Click **OK**.

To configure Mac clients to use an internal LiveUpdate server

1 Under **Policies**, click **LiveUpdate**.

2 On the **LiveUpdate Settings** tab, right-click the policy that you want and then click **Edit**.

3 Under **Mac Settings**, click **Server Settings**.

4 Click **Use a specified internal LiveUpdate server**, and then click **Add**.

5 In the **Add LiveUpdate Server** dialog box, type the information that you need to identify and communicate with the server that you want to use.

For example, for the URL:

■ If you use the FTP method (recommended), type the FTP address for the server. For example: ftp://myliveupdateserver.com

■ If you use the HTTP method, type the URL for the server. For example: http://myliveupdateserver.com or 2.168.133.11/Export/Home/LUDepot

6 If required, type in a user name and password for the server and then click **OK**.

7 If your server uses FTP, click **Advanced Server Settings**.

8 Click the FTP mode that the server uses, either **Active** or **Passive**, and then click **OK**.

9 If you use LiveUpdate Administrator version 1.x instead of the current version, click **Enable support for LiveUpdate Administrator version 1.x**.

10 Under **Mac Settings**, click **Advanced Settings**.

If you want to let client computers to get product update settings through LiveUpdate, click **Download Symantec Endpoint Protection product updates using a LiveUpdate server**.

11 Click **OK**.

See "Randomizing content downloads from a LiveUpdate server" on page 573.

See "Configuring client updates to run when client computers are idle" on page 574.

See "How client computers receive content updates" on page 554.

Using Group Update Providers to distribute content to clients

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

One advantage of Group Update Provider use is that it helps you to conserve bandwidth by offloading processing power from the server to the Group Update Provider. Group Update Providers are ideal for delivering content updates to clients that have limited network access to the server. You can use a Group Update Provider to conserve bandwidth to clients in a remote location over a slow link. Setting up a Group Update Provider is easier than setting up an internal LiveUpdate server. Group Update Providers are less resource-intensive and so reduce the load on the management servers.

You use a LiveUpdate Settings policy to configure Group Update Providers.

Table 24-6   Tasks to configure and use Group Update Providers

Step	Action	Description
Step 1	Understand the differences between the types of Group Update Providers that you can configure	A single Group Update Provider is a dedicated client computer that provides content for one or more groups of clients. Multiple Group Update Providers use a set of rules, or criteria, to elect themselves to serve groups of clients in their subnet. An explicit list of Group Update Providers lets clients connect to Group Update Providers that are on subnets other than the client's own subnet. You use the explicit list to map the single Group Update Providers and multiple Group Update Providers to the client subnets. The types of Group Update Provider that you choose to configure depends on your network and the clients on that network. See "About the types of Group Update Providers" on page 582. See "About the effects of configuring more than one type of Group Update Provider in your network" on page 586. See "About configuring rules for multiple Group Update Providers" on page 588.
Step 2	Verify client communication	Before you configure Group Update Providers, verify that the clients can receive content updates from the server. Resolve any client-server communication problems. You can view client-server activity in the System logs on the **Logs** tab of the **Monitors** page. See "Troubleshooting communication problems between the management server and the client" on page 756.
Step 3	Configure Group Update Providers in one or more LiveUpdate Settings policies	You configure Group Update Providers by specifying **Server Settings** in the LiveUpdate Settings policy. You can configure a single Group Update Provider, an explicit list of Group Update Providers, or multiple Group Update Providers. See "Configuring Group Update Providers" on page 589.
Step 4	Assign the LiveUpdate Settings policy to groups	You assign the LiveUpdate Settings policy to the groups that use the Group Update Providers. You also assign the policy to the group in which the Group Update Provider resides. For a single Group Update Provider, you assign one LiveUpdate Settings policy per group per site. For multiple Group Update Providers and explicit lists of Group Update Providers, you assign one LiveUpdate Settings policy to multiple groups across subnets. See "Assigning a policy to a group" on page 300.

Table 24-6		Tasks to configure and use Group Update Providers *(continued)*
Step	**Action**	**Description**
Step 5	Verify that clients are designated as Group Update Providers	You can view the client computers that are designated as Group Update Providers. You can search client computers to view a list of Group Update Providers. You can also click a client computer on the **Clients** page and view its properties to see whether or not it is a Group Update Provider. See "Searching for the clients that act as Group Update Providers" on page 593.

About the types of Group Update Providers

You can configure several different types of Group Update Providers in the LiveUpdate Settings policy: a single Group Update Provider, an explicit list of Group Update Providers, and multiple Group Update Providers. The types of Group Update Provider are not mutually exclusive. You can configure one or more type of Group Update Provider per policy.

- Single Group Update Provider
  A single Group Update Provider is a dedicated client computer that provides content for one or more groups of clients. A single Group Update Provider can be a client computer in any group. To configure a single Group Update Provider, you specify the IP address or host name of the client computer that you want to designate as the Group Update Provider. A single Group Update Provider is a static Group Update Provider.
  Configuring a single Group Update Provider turns a single client into a Group Update Provider.

- Explicit Group Update Providers list
  You can configure an explicit list of Group Update Providers that clients can use to connect to Group Update Providers that are on subnets other than the client's subnet. Clients that change location frequently can then roam to the closest Group Update Provider on the list.
  An explicit Group Update Providers list does not turn clients into Group Update Providers. You use an explicit Group Update Provider list to map the client subnet network addresses to the Group Update Providers. You identify the Group Update Providers by any of following means:

  - IP address

  - Host name

  - Subnet

  Explicit Group Update Providers can be static or dynamic, depending on how you configure them. If you use an IP address or a host name to configure an

explicit Group Update Provider, then it is a static Group Update Provider. This difference affects how Group Update Providers act in networks that mix legacy version clients and managers with clients and managers from the current release.

If you use a subnet to designate a Group Update Provider, it is dynamic, as clients search for a Group Update Provider on that subnet.

Note: This subnet is the Group Update Provider subnet network address, which is sometimes also referred to as the network prefix or network ID.

■ Multiple Group Update Providers list

Multiple Group Update Providers use a set of rules, or criteria, to elect themselves to serve groups of clients in their own subnets. To configure multiple Group Update Providers, you specify the criteria that client computers must meet to qualify as a Group Update Provider. You can use a host name or IP address, registry keys, or operating system as criteria. If a client computer meets the criteria, the Symantec Endpoint Protection Manager adds the client to a global list of Group Update Providers. Symantec Endpoint Protection Manager then makes the global list available to all the clients in the network. Clients check the list and choose the Group Update Providers that are located in their own subnet. Multiple Group Update Providers are dynamic Group Update Providers.

Configuring multiple Group Update Providers turns multiple clients into Group Update Providers.

Note: You cannot use multiple Group Update Providers with the legacy clients that run versions of Symantec Endpoint Protection earlier than version 11.0.5 (RU5).

Configuring single or multiple Group Update Providers in a LiveUpdate Settings policy performs the following functions:

■ It specifies which clients with this policy are to act as Group Update Providers.

■ It specifies which Group Update Provider or Providers the clients with this policy should use for content updates.

Configuring an Explicit Group Update Provider list performs only one function:

■ It specifies which Providers the clients with this policy should use for content updates. It maps Group Update Providers on subnets for use by clients on different subnets.

■ It does not specify any clients as Group Update Providers.

Although it does not turn clients into Group Update Providers, you can still configure and apply a policy that contains only an explicit provider list. However, you must then have a single Group Update Provider or multiple Group Update Providers configured in another policy in the Symantec Endpoint Protection Manager. Or, you can have both types configured in other policies.

Note: Because Symantec Endpoint Protection Manager constructs a global list, all of the Group Update Providers that are configured in any of the policies on a Symantec Endpoint Protection Manager are potentially available for clients' use. Clients on a different subnet can end up using a Group Update Provider that you configured as a single static provider if the configured subnet mapping in an explicit list in another policy matches it.

See "About the effects of configuring more than one type of Group Update Provider in your network" on page 586.

If a client cannot obtain its update through any of the Group Update Providers, it can then optionally try to update from the Symantec Endpoint Protection Manager.

Table 24-7 How the explicit type of Group Update Provider can be used based on the software versions in the network

Symantec Endpoint Protection Manager Version	Client Versions	Group Update Provider Client Version	Types of Group Update Provider that you can use
12.1.2 and higher	12.1.2 and higher	11.0.5 and higher	You can configure both static and dynamic explicit Group Update Providers.
12.1.2 and higher	12.1.2 and higher	11.0.0 to 11.0.4	You can configure an 11.0.4 client computer as a single Group Update Provider. You can then use it in an explicit Group Update Provider list as a static Group Update Provider.
12.1.2 and higher	12.1.1 and lower	Any	You can configure single or multiple Group Update Providers, but not explicit Group Update Providers because the clients do not support them.
12.1.1 and lower	Any	Any	You can configure single or multiple Group Update Providers, but not any type of explicit Group Update Provider because they are not available in the Symantec Endpoint Protection Manager.

The types of Group Update Providers that you configure depend on how your network is set up and whether your network includes legacy clients.

Note: A legacy client is considered a computer that runs a version of Symantec Endpoint Protection that is earlier than 11.0.5.

Table 24-8   When to use particular types of Group Update Provider

Group Update Provider Type	When to use
Single	Use a single Group Update Provider when your network includes any of the following scenarios: ■ Your network includes legacy clients Legacy clients can get content from a single Group Update Provider; legacy clients can also be designated as a Group Update Provider. Legacy clients do not support multiple Group Update Providers. ■ You want to use the same Group Update Provider for all your client computers You can use a single LiveUpdate Settings policy to specify a static IP address or host name for a single Group Update Provider. However, you must change the IP address in the policy if the clients that serve as single Group Update Providers change locations. If you want to use different single Group Update Providers in different groups, you must create a separate LiveUpdate Settings policy for each group.
Explicit list	Use an explicit list of Group Update Providers when you want clients to be able to connect to Group Update Providers that are on subnets other than the client's subnet. Clients that change location can roam to the closest Group Update Provider on the list. **Note:** Clients from releases earlier than this release do not support the use of explicit Group Update Provider lists. Clients that communicate with Symantec Endpoint Protection Manager versions 12.1 and earlier do not receive any information about explicit Group Update Provider lists.

| | Table 24-8 | When to use particular types of Group Update Provider *(continued)* |

Group Update Provider Type	When to use
Multiple	Use multiple Group Update Providers when your network includes any of the following scenarios: ■ The client computers on your network are not legacy clients. Multiple Group Update Providers are supported on the computers that run Symantec Endpoint Protection 11.0.5 (RU5) software or a later version. You cannot use multiple Group Update Providers with the legacy clients that run versions of Symantec Endpoint Protection earlier than 11.0.5 (RU5). Legacy clients cannot get content from multiple Group Update Providers. A legacy client cannot be designated as a Group Update Provider even if it meets the criteria for multiple Group Update Providers. You can create a separate LiveUpdate Settings policy and configure a single, static Group Update Provider for a group of legacy clients. ■ You have multiple groups and want to use different Group Update Providers for each group You can use one policy that specifies rules for the election of multiple Group Update Providers. If clients change locations, you do not have to update the LiveUpdate Settings policy. The Symantec Endpoint Protection Manager combines multiple Group Update Providers across sites and domains. It makes the list available to all clients in all groups in your network. ■ Multiple Group Update Providers can function as a failover mechanism. The use of Multiple Group Update Providers ensures a higher probability that at least one Group Update Provider is available in each subnet.

About the effects of configuring more than one type of Group Update Provider in your network

When you configure single or multiple Group Update Providers in policies, then Symantec Endpoint Protection Manager constructs a global list of all the providers that have checked in. By default, on 32-bit operating systems, this file is \Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\gup \globallist.xml. Symantec Endpoint Protection Manager provides this global list to any client that asks for it so that the client can determine which Group Update Provider it should use. Because of this process, clients that have policies with only multiple or explicit Group Update Providers configured can also use single Group Update Providers, if the single provider meets the explicit mapping criterion. This

phenomenon can occur because single providers are a part of the global list of providers that the clients get from their Symantec Endpoint Protection Manager.

So, all of the Group Update Providers that are configured in any of the policies on a Symantec Endpoint Protection Manager are potentially available for clients' use. If you apply a policy that contains only an explicit Group Update Provider list to the clients in a group, all of the clients in the group attempt to use the Group Update Providers that are in the Symantec Endpoint Protection Manager global Group Update Provider list that meet the explicit mapping criteria.

Note: A Symantec Endpoint Protection client may have multiple IP addresses. Symantec Endpoint Protection considers all IP addresses when it matches to a Group Update Provider. So, the IP address that the policy matches is not always bound to the interface that the client uses to communicate with the Symantec Endpoint Protection Manager and the Group Update Provider.

If all types of Group Update Providers are configured in the policies on a Symantec Endpoint Protection Manager, then clients try to connect to Group Update Providers in the global list in the following order:

- Providers on the **Multiple Group Update Providers** list, in order

- Providers on the **Explicit Group Update Providers** list, in order

- The Provider that is configured as a **Single Group Update Provider**

You can configure the following types of explicit mapping criteria:

- IP address: Clients in subnet A should use the Group Update Provider that has the IP address *x.x.x.x*.

- Host name: Clients in subnet A should use the Group Update Provider that has the host name *xxxx*.

- Subnet network address: Clients in subnet A should use any Group Update Provider that resides on *subnet B*.

Multiple mapping criteria can be used in an explicit Group Update Provider list in a single policy. Symantec recommends that you be very careful how you configure multiple mapping criteria to avoid unintended consequences. For example, you can strand your clients without a means of obtaining updates if you misconfigure an explicit mapping.

Consider a scenario with the following multiple explicit mapping criteria configured in a single policy:

- If a client is in subnet 10.1.2.0, use the Group Update Provider that has IP address 10.2.2.24

- If a client is in subnet 10.1.2.0, use the Group Update Provider that has IP address 10.2.2.25

- If a client is in subnet 10.1.2.0, use the Group Update Provider that has host name **SomeMachine**

- If a client is in subnet 10.1.2.0, use any Group Update Provider on subnet 10.5.12.0

- If a client is in subnet 10.6.1.0, use any Group Update Provider on subnet 10.10.10.0

With this explicit Group Update Provider policy, if a client is in subnet 10.1.2.0, the first four rules apply; the fifth rule does not. If the client is in a subnet for which no mapping is specified, such as 10.15.1.0, then none of the rules apply to that client. That client's policy says to use an explicit Group Update Provider list, but there is no mapping that the client can use based on these rules. If you also disabled that client's ability to download updates from Symantec Endpoint Protection Manager and the Symantec LiveUpdate server, then that client has no usable update method.

About configuring rules for multiple Group Update Providers

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

Rules are structured as follows:

- Rule sets
  A rule set includes the rules that a client must match to act as a Group Update Provider.

- Rules
  Rules can specify IP addresses, host names, Windows client registry keys, or client operating systems. You can include one of each rule type in a rule set.

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

Table 24-9   Rule types

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

Table 24-9 Rule types *(continued)*

Rule type	Description
Operating system	This rule specifies client operating systems.

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

- Multiple rule sets are OR'ed.
  A client must match at least one rule set to act as a Group Update Provider.

- Multiple rules are AND'ed.
  A client must match every rule that is specified in a rule set to act as a Group Update Provider.

- Multiple values for a rule condition are OR'ed.
  A client must match one of the values in a rule condition to act as a Group Update Provider.

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

Configuring Group Update Providers

You configure Group Update Providers in the LiveUpdate Settings policy.

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

You can configure the maximum amount of time that clients try to download updates from a Group Update Provider before they try to get updates from their default management server. If you set this time to 15 minutes, this means that the client computer must try to download continuously for 15 minutes with no success.

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

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

You can configure multiple Group Update Providers by specifying the criteria that clients use to determine if they qualify to act as a Group Update Provider.

You can configure an explicit list of Group Update Providers for roaming clients to use.

See "Using Group Update Providers to distribute content to clients " on page 580.

See "About the types of Group Update Providers" on page 582.

To configure a Group Update Provider

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

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

3   On the **LiveUpdate Settings** tab, right-click the policy that you want and then click **Edit**.

4   In the **LiveUpdate Settings Policy** window, click **Server Settings**.

5   Under **Internal or External LiveUpdate Server**, check **Use the default management server**.

6   Under **Group Update Provider**, check **Use a Group Update Provider**.

7   Click **Group Update Provider**.

8   Do one of the following tasks:

  ■ Follow the steps in To configure a single Group Update Provider.

  ■ Follow the steps in To configure multiple Group Update Providers.

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

9   In the **Group Update Provider** dialog box, configure the options to control
    how content is downloaded and stored on the Group Update Provider
    computer.

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

10 Click **OK**.

To configure a single Group Update Provider

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

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

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

3   Return to the procedure to configure a Group Update Provider.

To configure multiple Group Update Providers

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

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

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

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

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

    ■   **Computer IP Address or Host Name**

    ■   **Registry Keys**

    ■   **Operating System**

6   If you selected **Computer IP Address or Host Name** or **Registry Keys**, click
    Add.

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

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

    See "About configuring rules for multiple Group Update Providers"
    on page 588.

8 Click **OK** until you return to the **Group Update Provider List** dialog box, where you can optionally add more rule sets.

9 Click **OK**.

10 Return to the procedure to configure a Group Update Provider.

When you configure an explicit list of Group Update Providers, you can specify that Symantec Endpoint Protection clients with IP addresses that fall on a particular subnet should use a particular Group Update Provider. Note that a client may have multiple IP addresses and that Symantec Endpoint Protection considers all of its IP addresses when it matches the Group Update Provider to use. So, the IP address that the policy matches to is not necessarily bound to the interface that the client uses to communicate with the Group Update Provider.

For example, suppose that a client has IP address A, which it uses to communicate with the Symantec Endpoint Protection Manager and with the Group Update Provider. This same client also has IP address B, which is the one that matches the Explicit Group Update Provider that you have configured in the LiveUpdate Settings policy for this client. The client can choose to use a Group Update Provider based on the address B, even though that is not the address that it uses to communicate with the Group Update Provider.

To configure an explicit list of Group Update Providers

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

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

3 On the **LiveUpdate Settings** tab, click **Add a LiveUpdate Settings policy**, or right-click the policy that you want and then click **Edit**.

4 In the **LiveUpdate Settings Policy** window, click **Server Settings**.

5 Under **Internal or External LiveUpdate Server**, check **Use the default management server**.

6 Under **Group Update Provider**, check **Use a Group Update Provider**.

7 Click **Group Update Provider**.

8 In the **Group Update Provider** dialog box, under **Group Update Provider Selection for Client**, click **Explicit Group Update Providers for roaming clients**, and then click **Configure Explicit Group Update Provider List**.

9 Click **Add**.

10 In the **Add Explicit Group Update Provider** dialog box, type in the client subnet that you want to map these Group Update Providers to.

11 Under **Explicit Group Provider Settings**, select the **Type** of mapping you want to set up: based on the IP address, the host name, or the Group Update Provider's network address.

12 Type in the necessary settings for the type of mapping you selected, and then click **OK**.

Searching for the clients that act as Group Update Providers

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

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

To search for the clients that act as Group Update Providers

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

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

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

4 In the **Find** drop-down list , select **Computers**.

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

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

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

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

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

9 Click **Search**.

See "Using Group Update Providers to distribute content to clients " on page 580.

Using Intelligent Updater files to update client virus and security risk definitions

Symantec recommends that client computers use LiveUpdate to update virus and security risk definitions. However, if you do not want to use LiveUpdate or if LiveUpdate is not available, you can use an Intelligent Updater file to update clients. The Intelligent Updater .exe files are designed to update clients only.

Intelligent Updater files do not contain the information that a Symantec Endpoint Protection Manager or a legacy Symantec AntiVirus parent server needs to update its managed clients.

An Intelligent Updater file is a self-executing file that contains virus and spyware definitions updates. An Intelligent Updater file does not provide updates for any other type of content. After you download the file, you can use your preferred distribution method to distribute the updates to your clients.

Note: Intelligent Updater does not support the Extended file attributes and signatures or the Auto-Protect portal list.

To download an Intelligent Updater file

1   Using your Web browser, go to one of the following sites:

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

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

2   On the Web site or on the FTP site, click the appropriate product file with the .exe extension.

3   When you are prompted for a location in which to save the file, select a folder on your hard drive.

4   Distribute the file to the client computers using your preferred distribution method.

To install the virus and security risk definitions files on a client computer

1   On the client computer, locate the Intelligent Updater file that was distributed to the client.

2   Double-click the .exe file and follow the on-screen instructions.

See "How client computers receive content updates" on page 554.

Using third-party distribution tools to update client computers

Some large enterprises rely on third-party distribution tools like IBM Tivoli or Microsoft SMS to distribute content updates to client computers. Symantec Endpoint Protection supports the use of third-party distribution tools to update the managed and unmanaged clients that run Windows operating systems. Mac clients can only receive content updates from internal or external LiveUpdate servers.

Table 24-10 outlines the tasks that you need to perform to use a third-party distribution tool.

Note: Before you set up the use of third-party distribution tools, you must have already installed Symantec Endpoint Protection Manager and the client computers that you want to update.

Table 24-10 Tasks to set up the use of third-party distribution tools for updates

Task	Description
Configure Symantec Endpoint Protection Manager to receive content updates.	You can configure the management server either to receive content updates automatically or manually. See "Configuring a site to download content updates" on page 559. See "Managing content updates" on page 546.
Configure the group's LiveUpdate Settings policy to allow third-party content update distribution.	If you want to use third-party distribution tools to update managed clients, you must configure the group's LiveUpdate Settings policy to allow it. See "Configuring a LiveUpdate Settings policy to allow third-party content distribution to managed clients" on page 596.
Prepare unmanaged clients to receive updates from third-party distribution tools.	If you want to use third-party distribution tools to update unmanaged clients, you must first create a registry key on each unmanaged client. See "Preparing unmanaged clients to receive updates from third-party distribution tools" on page 597.
Locate, copy, and distribute the content.	Each Symantec Endpoint Protection Manager client group has an index2.dax file that is located on the computer that runs Symantec Endpoint Protection Manager. These files are located in subfolders under the *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent folder. To update clients, you need to use the index2.dax files. See "Configuring a site to download content updates" on page 559. See "Distributing the content using third-party distribution tools" on page 598.

Configuring a LiveUpdate Settings policy to allow third-party content distribution to managed clients

If you want to use third-party distribution tools to update managed clients, you must configure the client group's LiveUpdate Settings policy to allow it. You can choose whether to disable the ability of client users to manually perform LiveUpdate.

When you are finished with this procedure, a folder appears on the group's client computers in the following locations:

■ Pre-Vista operating systems, Symantec Endpoint Protection 11.x legacy clients: *drive*:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\inbox

■ Vista operating systems, Symantec Endpoint Protection 11.x legacy clients: *drive*:\Program Data\Symantec\Symantec Endpoint Protection\inbox

■ Pre-Vista operating systems, version 12.1 Symantec Endpoint Protection clients
drive:\Documents and Settings\All Users\Application Data\Symantec\CurrentVersion\inbox

■ Vista operating systems, version 12.1 Symantec Endpoint Protection clients
drive:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox

To enable third-party content distribution to managed clients with a LiveUpdate policy

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

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

3 On the **LiveUpdate Settings** tab, under **Tasks**, click **Add a LiveUpdate Setting Policy**.

4 In the **LiveUpdate Policy** window, in the **Policy name** and **Description** text boxes, type a name and description.

5 Under **Windows Settings**, click **Server Settings**.

6 Under **Third Party Management**, check **Enable third party content management**.

7 Uncheck all other LiveUpdate source options.

8 Click **OK**.

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

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

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

See "Setting up an internal LiveUpdate server" on page 577.

Preparing unmanaged clients to receive updates from third-party distribution tools

If you install unmanaged clients from the product disc, you cannot immediately use third-party distribution tools to distribute LiveUpdate content or policy updates to them. As a security measure, by default these client computers do not trust or process the content that third-party distribution tools deliver to them.

To successfully use third-party distribution tools to deliver updates, you must first create a Windows registry key on each of the unmanaged clients. The key lets you use the inbox folder on unmanaged clients to distribute LiveUpdate content and policy updates by using third-party distribution tools.

The inbox folder appears on unmanaged clients in the following locations:

■ Pre-Vista operating systems, legacy clients:
   drive:\Documents and Settings\All Users\Application Data\Symantec\Symantec Endpoint Protection\inbox

■ Vista operating systems, legacy clients:
   drive:\Program Data\Symantec\Symantec Endpoint Protection\inbox

■ Pre-Vista operating systems, version 12.1 Symantec Endpoint Protection clients
   drive:\Documents and Settings\All Users\Application Data\Symantec\CurrentVersion\inbox

■ Vista operating systems, version 12.1 Symantec Endpoint Protection clients
   drive:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox

Once you create the registry key, you can use a third-party distribution tool to copy content or policy updates to this folder. The Symantec Endpoint Protection client software then trusts and processes the updates.

To prepare unmanaged clients to receive updates from third-party distribution tools

1   On each client computer, use regedit.exe or another Windows registry editing tool to create one of the following Windows registry keys:

■ On the clients that run Symantec Endpoint Protection 12.1, create **HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState**

■ On the clients that run Symantec Endpoint Protection 11.x, create **HKLM\Software\Symantec\Symantec Endpoint Protection\SMC\TPMState**

2   Set the value of the registry key to hexadecimal 80, as follows:

    ```
    0x00000080 (128)
    ```

Note: The value is of type DWORD.

---

3   Save the registry key, and then exit the registry editing tool.

See "Using third-party distribution tools to update client computers" on page 594.

See "Distributing the content using third-party distribution tools" on page 598.

Distributing the content using third-party distribution tools

To use third-party distribution tools to distribute content to client computers, you need to use the index2.dax file. The LiveUpdate-related content in the index2 file includes a set of GUIDs called content monikers and their associated sequence numbers. Each content moniker corresponds to a particular content type. Each sequence number in the index2 file corresponds to a revision of a particular content type. Depending on the protection features that you have installed, you need to determine which of the content types you need.

See "About the types of content that LiveUpdate can provide" on page 549.

Content moniker mapping for updating legacy clients

Except for virus and spyware definitions, which are backwards compatible with Symantec Endpoint Protection 11.x releases, this content is for clients that run the current release of Symantec Endpoint Protection. If you have legacy clients to update with other types of content, you should use legacy content to update them. This method of using third-party management tools cannot be used to update clients running Symantec AntiVirus or Symantec Client Security releases prior to Symantec Endpoint Protection 11.x releases.

Note: Content monikers typically change with each major release. At times, they may also change for a minor release. Symantec does not typically change the monikers for Release Updates or Maintenance Patches.

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

For example, you might see the following entry:

```
{535CB6A4-441F-4e8a-A897-804CD859100E}: SESC Virus Definitions
Win32 v11 - MicroDefsB.CurDefs - SymAllLanguages
```

Each Symantec Endpoint Protection Manager client group has its own index2 file. The index2 file for each client group is found in a folder for that group. The folders for client groups can be found in *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent. The folder name for a client group corresponds to the group policy serial number. You can find the serial number in the **Group Properties** dialog box or on the **Clients** page **Details** tab. The first four hexadecimal values of each group policy serial number match the first four hexadecimal values of that group's folder.

The index2.dax file that managed clients use is encrypted. To look at the contents of the file, open the index2.xml file that is available in the same folder. The index2.xml file provides a list of the content monikers and their sequence (revision) numbers. For example, you might see the following entry:

```
<File Checksum="191DEE487AA01C3EDA491418B53C0ECC" DeltaFlag="1"
FullSize="30266080" LastModifiedTime="1186471722609" Moniker=
"{535CB6A4-441F-4e8a-A897-804CD859100E}" Seq="80806003"/>
```

The LiveUpdate Content policy for a group specifies either a particular revision of content or the latest content. The sequence number in the index2 file must match the sequence number that corresponds to the content specification in the group's LiveUpdate Content policy. For example, if the policy is configured to **Use latest available** for all content types, then the sequence number for each type is the latest available content. In this example, the distribution only works if the index2 file calls out the sequence numbers (revisions) that correspond to the latest content revision. The distribution fails if the sequence numbers correspond to any other revisions.

> **Note:** You must use the Copy command to place files into the client's \inbox folder. Using the Move command does not trigger update processing, and the update fails. If you compress content into a single archive for distribution, you should not unzip it directly into the \inbox folder.

If you distribute virus and spyware content to legacy clients that use Symantec Endpoint Protection 11.x, the moniker scheme has changed. You can use the 12.x definitions to update legacy clients, but you must rename the target moniker before you distribute them.

To distribute content to clients with third-party distribution tools

1   On the computer that runs the Symantec Endpoint Protection Manager, create a working folder such as \Work_Dir.

2   Do one of the following actions:

   ■   For a managed client, in the console, on the **Clients** tab, right-click the group to update, and then click **Properties**.

   ■   For an unmanaged client, in the console, on the **Clients** tab, right-click **My Company**, and then click **Properties**.

3   Write down the first four hexadecimal values of the **Policy Serial Number**, such as 7B86.

4   Navigate to the following folder:

   \\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent

5   Locate the folder that contains the first four hexadecimal values that match the **Policy Serial Number**.

6   Open that folder, and then copy the `index2.dax` file to your working folder.

7   Navigate to the following folder:

   \\Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\content

8   Open and read `ContentInfo.txt` to discover the content that each *target moniker* folder contains.

   The contents of each directory is *target moniker\sequence number*full.zip|full.

9   Copy the contents of each *target moniker* folder to your working folder such as \Work_Dir.

10   To distribute virus and spyware definitions content to Symantec Endpoint Protection 11.x legacy clients, you must take the following steps:

- For 32-bit computers, copy the
  {535CB6A4-441F-4e8a-A897-804CD859100E}*sequence number*\full.zip
  contents.
  Rename the contents to
  {C60DC234-65F9-4674-94AE-62158EFCA433}*sequence number*\full.zip,
  then copy the contents to your working folder.

- For 64-bit computers, copy the
  {07B590B3-9282-482f-BBAA-6D515D385869}*sequence number*\full.zip
  contents.
  Rename the contents to
  {1CD85198-26C6-4bac-8C72-5D34B025DE35}*sequence number*\full.zip,
  then copy the contents to your working folder.

11 Delete all files and folders from each *target moniker* so that only the following
   folder structure and file remain in your working folder:

   \\\\Work_Dir*target moniker**latest sequence number*\full.zip

   Your working folder now contains the folder structure and files to distribute
   to your clients.

12 Use your third-party distribution tools to distribute the content of your
   working folder to the \\\\Symantec Endpoint Protection\inbox\ folder on each
   of the clients.

   The end result must look like the following:

   \\\\Symantec Endpoint Protection\inbox\index2.dax

   \\\\Symantec Endpoint Protection\inbox*target moniker**latest sequence
   number*\full.zip

   Files that are processed successfully are then deleted. Files that are not
   processed successfully are moved to a subfolder named Invalid. If you see
   files in an **Invalid** folder under the **inbox** folder, then you must try again with
   those files.

See "Using third-party distribution tools to update client computers" on page 594.

See "Preparing unmanaged clients to receive updates from third-party distribution
tools" on page 597.

Monitoring protection with reports and logs

This chapter includes the following topics:

- Monitoring endpoint protection
- Configuring reporting preferences
- Logging on to reporting from a stand-alone Web browser
- About the types of reports
- Running and customizing quick reports
- Saving and deleting custom reports
- Creating scheduled reports
- Editing the filter used for a scheduled report
- Printing and saving a copy of a report
- Viewing logs
- Running commands from the computer status log

Monitoring endpoint protection

Symantec Endpoint Protection collects information about the security events in your network. You can use log and reports to view these events, and you can use notifications to stay informed about the events as they occur.

You can use the reports and logs to determine the answers to the following kinds of questions:

- Which computers are infected?

- Which computers need scanning?

- What risks were detected in the network?

Note: Symantec Endpoint Protection pulls the events that appear in the reports from the event logs on your management servers. The event logs contain time-stamps in the client computers' time zones. When the management server receives the events, it converts the event time-stamps to Greenwich Mean Time (GMT) for insertion into the database. When you create reports, the reporting software displays information about events in the local time of the computer on which you view the reports.

Table 25-1   Tasks for monitoring endpoint protection

Task	Description
Review the security status of your network	The following list describes some of the tasks that you can perform to monitor the security status of your client computers.

The following list describes some of the tasks that you can perform to monitor the security status of your client computers.

- Obtain a count of detected viruses and other security risks and view details for each virus and security risk.
  See "Viewing risks" on page 610.
- Obtain a count of unprotected computers in your network and view the details for each computer.
  See "Viewing system protection" on page 608.
- View the number of computers with up-to-date virus and spyware definitions.
  See "Viewing system protection" on page 608.
- View the real-time operational status of your client computers.
  See "Viewing the protection status of clients and client computers" on page 226.
- View the number of computers that are offline.
  See "Finding offline computers" on page 609.
- Review the processes that run in your network.
  See "Monitoring SONAR detection results to check for false positives" on page 404.
- Locate which computers are assigned to which groups.
- View a list of the Symantec Endpoint Protection software versions that are installed on the clients and Symantec Endpoint Protection Manager servers in your network.
  See "Generating a list of the Symantec Endpoint Protection versions installed on the clients and servers in your network" on page 613.
- View the licensing information on the client computers, which includes the number of valid seats, over-deployed seats, expired seats, and expiration date.
  See "Checking license status" on page 119.

See "Viewing the status of deployed client computers" on page 611.

See "Viewing a daily or weekly status report" on page 608.

| Locate which client computers need protection | You can perform the following tasks to view or find which computers need additional protection: |

You can perform the following tasks to view or find which computers need additional protection:

- View the number of computers with Symantec Endpoint Protection disabled.
  See "Viewing system protection" on page 608.
- View the number of computers with out-of-date virus and spyware definitions.
  See "Viewing system protection" on page 608.
- Find the computers that have not been scanned recently.
  See "Finding unscanned computers" on page 609.
- View attack targets and sources.
  See "Viewing attack targets and sources" on page 612.
- View event logs.
  See "Viewing logs" on page 624.

Table 25-1 Tasks for monitoring endpoint protection *(continued)*

Task	Description
Protect your client computers	You can run commands from the console to protect the client computers. See "Running commands from the computer status log" on page 630. For example, you can eliminate security risks on client computers. See "Checking the scan action and rescanning the identified computers" on page 322.
Configure notifications to alert you when security events occur	You can create and configure notifications to be triggered when certain security-related events occur. For example, you can set a notification to occur when an intrusion attempt occurs on a client computer. See "Setting up administrator notifications" on page 642.
Create custom quick reports and scheduled reports for ongoing monitoring	You can create and generate customized quick reports and you can schedule custom reports to run regularly with the information that you want to see. See "Running and customizing quick reports" on page 618. See "Creating scheduled reports" on page 621. See "Saving and deleting custom reports" on page 620. See "Configuring reporting preferences" on page 613.

Table 25-1   Tasks for monitoring endpoint protection *(continued)*

Task	Description
Minimize the amount of space that client logs take	For security purposes, you might need to retain log records for a longer period of time. However, if you have a large number of clients, you may have a large volume of client log data. If your management server runs low on space, you might need to decrease the log sizes, and the amount of time the database keeps the logs. You can reduce the volume of log data by performing the following tasks: ■ Upload only some of the client logs to the server, and change the frequency with which the client logs are uploaded. See "Specifying client log size and which logs to upload to the management server" on page 731. ■ Specify how many log entries the client computer can keep in the database, and how long to keep them. See "Specifying how long to keep log entries in the database" on page 732. ■ Filter the less important risk events and system events out so that less data is forwarded to the server. See "Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers" on page 386. ■ Reduce the number of clients that each management server manages. ■ Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server. See "Configuring push mode or pull mode to update client policies and content" on page 308. ■ Reduce the amount of space in the directory where the log data is stored before being inserted into the database. See "About increasing the disk space on the server for client log data" on page 733.
Export log data to a centralized location	Log data export is useful if you want to accumulate all logs from your entire network in a centralized location. Log data export is also useful if you want to use a third-party program such as a spreadsheet to organize or manipulate the data. You also might want to export the data in your logs before you delete log records. You can export the data in some logs to a comma-delimited text file. You can export other logs' data to a tab-delimited text file that is called a dump file or to a Syslog server. See "Exporting log data to a text file" on page 729. See "Exporting data to a Syslog server" on page 728. See "Exporting log data to a comma-delimited text file" on page 731. See "Viewing logs from other sites" on page 630.

Task	Description
Troubleshoot issues with reports and logs	You can troubleshoot some issues with reporting. See "Troubleshooting reporting issues" on page 771.

Viewing a daily or weekly status report

The Daily Status Report provides the following information:

- Virus detection counts for cleaned, suspicious, blocked, quarantined, deleted, newly infected, and still infected actions.

- Virus definition distribution timeline

- Top ten risks and infections

The Weekly Status Report provides the following information:

- Computer status

- Virus detection

- Protection status snapshot

- Virus definition distribution timeline

- Risk distribution by day

- Top ten risks and infections

See "Monitoring endpoint protection" on page 603.

To view the daily status report

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

2   On the **Home** page, in the **Favorite Reports** pane, click **Symantec Endpoint Protection Daily Status** or **Symantec Endpoint Protection Weekly Status**.

Viewing system protection

System protection comprises the following information:

- The number of computers with up-to-date virus definitions.

- The number of computers with out-of-date virus definitions.

- The number of computers that are offline.

- The number of computers that are disabled.

See "Monitoring endpoint protection" on page 603.

To view system protection

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

    System protection is shown in the **Endpoint Status** pane.

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

Finding offline computers

You can list the computers that are offline.

A client may be offline for a number of reasons. You can identify the computers
that are offline and remediate these problems in a number of ways.

See "Troubleshooting communication problems between the management server
and the client" on page 756.

To find offline computers

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

2   On the **Home** page, in the **Endpoint Status** pane, click the link that represents
    the number of offline computers.

3   To get more information about offline computers, click the **View Details** link.

To view offline client computers in the Computer Status log

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

2   On the **Logs** tab, from the **Log type** list box, click **Computer Status**.

3   Click **Advanced Settings**.

4   In the Online status list box, click **Offline**.

5   Click **View Log**.

    By default, a list of the computers that have been offline for the past 24 hours
    appears. The list includes each computer's name, IP address, and the last time
    that it checked in with its server. You can adjust the time range to display
    offline computers for any time range you want to see.

Finding unscanned computers

You can list the computers that need scanning.

See "Monitoring endpoint protection" on page 603.

To find unscanned computers

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

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

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

3   Click **Create Report**.

Viewing risks

You can get information about the risks in your network.

See "Monitoring endpoint protection" on page 603.

To view infected and at risk computers

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

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

Report type	**Risk**
Selected report	**Infected and At Risk Computers**

3   Click **Create Report**.

To better understand the benefits and risks of not enabling certain features, you can run the Risk Distribution by Protection Technology report. This report provides the following information:

- Signature-based detections of virus and spyware
- SONAR detections
- Download Insight detections
- Intrusion Prevention and browser protection detections

To view the risks detected by the types of protection technology

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

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

Report type   **Risk**

Selected report   **Risk Distribution by Protection Technology**

3   Click **Create Report**.

To view newly detected risks

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

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

Report type   **Risk**

Selected report   **New Risks Detected in the Network**

3   Click **Create Report**.

To view a comprehensive risk report

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

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

Report type   **Risk**

Select a report   **Comprehensive Risk Report**

3   Click **Create Report**.

Viewing the status of deployed client computers

You can confirm the status of your deployed client computers.

See "Monitoring endpoint protection" on page 603.

To view status of deployed client computers

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

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

Report type   **Computer Status**

Select a report   **Client Inventory Details**

3   Click **Create Report**.

Viewing attack targets and sources

You can view attack targets and sources.

See "Monitoring endpoint protection" on page 603.

To view the top targets that were attacked

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

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

Report type   You select **Network Threat Protection**.

Select a report   You select **Top Targets Attacked**.

3   Click **Create Report**.

To view top attack sources

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

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

Report type   You select **Network Threat Protection**.

Select a report   You select **Top Sources of Attack**.

3   Click **Create Report**.

A full report contains the following statistics:

■   Top attack types

■   Top targets of attack

■   Top sources of attack

■   Top traffic notifications

To view a full report on attack targets and sources

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

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

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

3   Click **Create Report**.

Generating a list of the Symantec Endpoint Protection versions installed on the clients and servers in your network

You can run a quick report from Symantec Endpoint Protection Manager that provides a list of the Symantec Endpoint Protection software versions that are installed on the clients and Symantec Endpoint Protection Manager servers in your network. This list can be useful when you want to upgrade or migrate your software from a previous version of Symantec Endpoint Protection. The list includes local and remote computers.

You can save the report using MHTML Web page archive format.

See

If you use Symantec Network Access Control, those software versions are also included in the report.

To generate a report that lists the Symantec Endpoint Protection software versions

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

2   For **Report type**, select **Computer Status**.

3   For **Select a report**, select **Symantec Endpoint Protection Product Versions**.

4   Click **Create Report**.

Configuring reporting preferences

You can configure the following reporting preferences:

■   The **Home** and **Monitors** pages display options

■   The **Security Status** thresholds

- The display options that are used for the logs and the reports, as well as legacy log file uploading

The security status thresholds that you set determine when the Security Status message on the Symantec Endpoint Protection Manager **Home** page is considered Poor. Thresholds are expressed as a percentage and reflect when your network is considered to be out of compliance with your security policies.

For example, you can set the percentage of computers with out-of-date virus definitions that triggers a poor security status. You can also set how many days old the definitions need to be to qualify as out of date. Symantec Endpoint Protection determines what is current when it calculates whether signatures or definitions are out of date as follows. Its standard is the most current virus definitions and IPS signature dates that are available on the management server on which the console runs.

Note: If you have only Symantec Network Access Control installed, you do not have a Security Status tab for configuring security thresholds.

For information about the preference options that you can set, you can click **Help** on each tab in the **Preferences** dialog box.

To configure reporting preferences

1   In the console, on the **Home** page, click **Preferences**.

2   Click one of the following tabs, depending on the type of preferences that you want to set:

   - **Home and Monitors**

   - **Security Status**

   - **Logs and Reports**

3   Set the values for the options that you want to change.

4   Click **OK**.

Logging on to reporting from a stand-alone Web browser

You can access the **Home**, **Monitors**, and **Reports** pages from a stand-alone Web browser that is connected to your management server. However, all of the other console functions are not available when you use a stand-alone browser.

Report pages and log pages always display in the language that the management server was installed with. To display these pages when you use a remote console or browser, you must have the appropriate font installed on the computer that you use.

To access reporting from a Web browser, you must have the following information:

■ The host name of the management server.

Note: When you type the HTTPS standalone reporting URL in your browser, the browser might display a warning. The warning appears because the certificate that the management server uses is self-signed. To work around this issue, you can install the certificate in your browser's trusted certificate store. The certificate supports host names only, so use the host name in the URL. If you use localhost, IP address, or the fully qualified domain name, a warning still appears.

■ Your user name and password for the management server.

Note: You must have Internet Explorer 6.0 or later installed. Other Web browsers are not supported.

To log on to reporting from a stand-alone Web browser

1   Open a Web browser.

2   Type the default reporting URL into the address text box in the following format:

https://*management server host name*:8445/reporting

Note: The Symantec Endpoint Protection version 11 default reporting URL is **http://*management server address*:8014/reporting**. If you migrate from version 11, you must update your browser's bookmarks.

3   When the logon dialog box appears, type your user name and password, and then click **Log On**.

If you have more than one domain, in the **Domain** text box, type your domain name.

About the types of reports

The following categories of reports are available:

- Quick reports, which you run on demand.
- Scheduled reports, which run automatically based on a schedule that you configure.

Reports include the event data that is collected from your management servers as well as from the client computers that communicate with those servers. You can customize reports to provide the information that you want to see.

The quick reports are predefined, but you can customize them and save the filters that you used to create the customized reports. You can use the custom filters to create custom scheduled reports. When you schedule a report to run, you can configure it to be emailed to one or more recipients.

See "Running and customizing quick reports" on page 618.

A scheduled report always runs by default. You can change the settings for any scheduled report that has not yet run. You can also delete a single scheduled report or all of the scheduled reports.

See "Creating scheduled reports" on page 621.

You can also print and save reports.

See "Printing and saving a copy of a report" on page 623.

Table 25-2 describes the types of reports that are available.

Table 25-2   Report types available as quick reports and scheduled reports

Report type	Description
Audit	Displays the information about the policies that clients and locations use currently. It includes information about policy modification activities, such as the event times and types, policy modifications, domains, sites, administrators, and descriptions.
Application and Device Control	Displays the information about events where some type of behavior was blocked. These reports include information about application security alerts, blocked targets, and blocked devices. Blocked targets can be Windows registry keys, dlls, files, and processes.

Table 25-2   Report types available as quick reports and scheduled reports
(continued)

Report type	Description
Compliance	Displays the information about the compliance status of your network. These reports include information about Enforcer servers, Enforcer clients, Enforcer traffic, and host compliance.
Computer Status	Displays the information about the operational status of the computers in your network, such as which computers have security features turned off. These reports include information about versions, the clients that have not checked in to the server, client inventory, and online status.
Network Threat Protection	Displays the information about intrusion prevention, attacks on the firewall, and about firewall traffic and packets. The Network Threat Protection reports let you track a computer's activity and its interaction with other computers and networks. They record information about the traffic that tries to enter or exit the computers through their network connections.
Risk	Displays the information about risk events on your management servers and their clients. It includes information about SONAR scans and, if you have legacy clients in your network, about TruScan proactive threat scans.
Scan	Displays the information about virus and spyware scan activity.
System	Displays the information about event times, event types, sites, domains, servers, and severity levels. The System reports contain information that is useful for troubleshooting client problems.

If you have multiple domains in your network, many reports let you view data for all domains, one site, or a few sites. The default for all quick reports is to show all domains, groups, servers, and so on, as appropriate for the report you select to create.

Note: Some predefined reports contain information that is obtained from Symantec Network Access Control. If you have not purchased that product, but you run one of that product's reports, the report is empty. If you have only Symantec Network Access Control installed, a significant number of reports are empty. The **Application and Device Control**, **Network Threat Protection**, **Risk**, and **Scan** reports do not contain data. The **Compliance** and **Audit** reports do contain data, as do some of the **Computer Status** and **System** reports.

Running and customizing quick reports

Quick reports are predefined, customizable reports. These reports include event data collected from your management servers as well as the client computers that communicate with those servers. Quick reports provide information on events specific to the settings you configure for the report. You can save the report settings so that you can run the same report at a later date, and you can print and save reports.

Quick reports are static; they provide information specific to the time frame you specify for the report. Alternately, you can monitor events in real time using the logs.

To run 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 run.

3   In the **Select a report** list box, select the name of the report you want to run.

4   Click **Create Report**.

To customize 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 customize.

3 In the **Select a report** list box, select the name of the report you want to customize.

For the **Network Compliance Status** report and the **Compliance Status** report, in the **Status** list box, select a saved filter configuration that you want to use, or leave the default filter.

For the **Top Risk Detections Correlation** report, you can select values for the **X-axis** and **Y-axis** list boxes to specify how you want to view the report.

For the **Scan Statistics Histogram Scan** report, you can select values for **Bin width** and **Number of bins**.

For some reports, you can specify how to group the report results in the **Group** list box. For other reports, you can select a target in the **Target** field on which to filter report results.

4 In the **Use a saved filter** list box, select a saved filter configuration that you want to use, or leave the default filter.

5 Under **What filter settings would you like to use?**, in the **Time range** list box, select the time range for the report.

6 If you select **Set specific dates**, then use the **Start date** and **End date** list boxes. These options set the time interval that you want to view information about.

When you generate a Computer Status report and select **Set specific dates**, you specify that you want to see all entries that involve a computer that has not checked in with its server since the time you specify in the date and time fields.

7 If you want to configure additional settings for the report, click **Advanced Settings** and set the options that you want.

You can click **Tell me more** to see descriptions of the filter options in the context-sensitive help.

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.

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**.

See "Saving and deleting custom reports" on page 620.

See "Printing and saving a copy of a report" on page 623.

Saving and deleting custom reports

You can save custom report settings in a filter so that you can generate the report again at a later date. When you save your settings, they are saved in the database. The name that you give to the filter appears in the **Use a saved filter** list box for that type of logs and reports.

Note: The filter configuration settings that you save are available for your user logon account only. Other users with reporting privileges do not have access to your saved settings.

You can delete any report configuration that you create. When you delete a configuration, the report is no longer available. The default report configuration name appears in the **Use a saved report** list box and the screen is repopulated with the default configuration settings.

Note: If you delete an administrator from the management server, you have the option to save the reports that were created by the deleted administrator. The ownership of the reports is changed, and the report names are changed. The new report name is in the format `"OriginalName('AdminName')"`. For example, a report that was created by administrator **JSmith**, named `Monday_risk_reports`, would be renamed `Monday_risk_reports(JSmith)`.

To save a custom report

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

2   On the **Quick Reports** tab, select a report type from the list box.

3   Change any basic settings or advanced settings for the report.

4   Click **Save Filter**.

5   In the **Filter name** text box, type a descriptive name for this report filter. Only the first 32 characters of the name that you give display when the filter is added to the **Use a saved filter** list.

6   Click **OK**.

7   When the confirmation dialog box appears, click **OK**.

   After you save a filter, it appears in the **Use a saved filter** list box for related
   reports and logs.

To delete a custom report

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

2   On the **Quick Reports** tab, select a report type.

3   In the **Use saved filter** list box, select the name of the filter that you want to
   delete.

4   Click the **Delete** icon beside the **Use a saved filter** list box.

5   When the confirmation dialog box appears, click **Yes**.

Creating scheduled reports

Scheduled reports are the reports that run automatically based on the schedule
that you configure. Scheduled reports are emailed to recipients, so you must
include the email address of at least one recipient. After a report runs, the report
is emailed to the recipients that you configure as an .mht file attachment.

The data that appears in the scheduled reports is updated in the database every
hour. At the time that the management server emails a scheduled report, the data
in the report is current to within one hour.

The other reports that contain data over time are updated in the database based
on the upload interval that you configured for the client logs.

See "Specifying client log size and which logs to upload to the management server"
on page 731.

Note: If you have multiple servers within a site that share a database, only the
first-installed server runs the reports scheduled for the site. This default ensures
that all the servers in the site do not run the same scheduled scans simultaneously.
If you want to designate a different server to run scheduled reports, you can
configure this option in the local site properties.

To create a scheduled report

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

2   On the **Scheduled Reports** tab, click **Add**.

3 In the **Report name** text box, type a descriptive name and optionally, type a longer description.

Although you can paste more than 255 characters into the description text box, only 255 characters are saved in the description.

4 If you do not want this report to run until another time, uncheck the **Enable this scheduled report** check box.

5 Select the report type that you want to schedule from the list box.

6 Select the name of the specific report that you want to schedule from the list box.

7 Select the name of the saved filter that you want to use from the list box.

8 In the **Run every** text box, select the time interval at which you want the report to be emailed to recipients (hours, days, weeks, months). Then, type the value for the time interval you selected. For example, if you want the report to be sent to you every other day, select days and then type 2.

9 In the **Start after** text box, type the date that you want the report to start or click the calendar icon and select the date. Then, select the hour and minute from the list boxes.

10 Under **Report Recipients**, type one or more comma-separated email addresses.

You must already have set up mail server properties for email notifications to work.

11 Click **OK** to save the scheduled report configuration.

Editing the filter used for a scheduled report

You can change the settings for any report that you have already scheduled. The next time the report runs it uses the new filter settings. You can also create additional scheduled reports, which you can base on a previously saved report filter.

Filter storage is based in part on the creator, so problems do not occur when two different users create a filter with the same name. However, an individual user or two users who log on to the default admin account should not create filters with the same name.

If users create filters with the same name, a conflict can occur under two conditions:

■ Two users are logged on to the default admin account on different sites and each creates a filter with the same name.

■ One user creates a filter, logs on to a different site, and immediately creates a filter with the same name.

If either condition occurs before site replication takes place, the user subsequently sees two filters with the same name in the filter list. Only one of the filters is usable. If this problem occurs, it is a best practice to delete the usable filter and recreate it with a different name. When you delete the usable filter, you also delete the unusable filter.

See "Saving and deleting custom reports" on page 620.

Note: When you associate a saved filter with a scheduled report, make sure that the filter does not contain custom dates. If the filter specifies a custom date, you get the same report every time the report runs.

See "Creating scheduled reports" on page 621.

To edit the filter used for a scheduled report

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

2   Click **Scheduled Reports**.

3   In the list of reports, click the scheduled report that you want to edit.

4   Click **Edit Filter**.

5   Make the filter changes that you want.

6   Click **Save Filter**.

    If you want to retain the original report filter, give this edited filter a new name.

7   Click **OK**.

8   When the confirmation dialog box appears, click **OK**.

Printing and saving a copy of a report

You can print a report or save a copy of a Quick Report. You cannot print scheduled reports. A saved file or printed report provides a snapshot of the current data in your reporting database so that you can retain a historical record.

Note: By default, Internet Explorer does not print background colors and images. If this printing option is disabled, the printed report may look different from the report that you created. You can change the settings in your browser to print background colors and images.

To print a copy of a report

1   In the report window, click **Print**.

2   In the **Print** dialog box, select the printer you want, if necessary, and then click **Print**.

When you save a report, you save a snapshot of your security environment that is based on the current data in your reporting database. If you run the same report later, based on the same filter configuration, the new report shows different data.

To save a copy of a report

1   In the report window, click **Save**.

2   In the **File Download** dialog box, click **Save**.

3   In the **Save As** dialog box, in the **Save in selection** dialog box, browse to the location where you want to save the file.

4   In the **File name** list box, change the default file name, if desired.

5   Click **Save**.

    The report is saved in MHTML Web page archive format in the location you selected.

6   In the **Download complete** dialog box, click **Close**.

Viewing logs

You can generate a list of events to view from your logs that are based on a collection of filter settings that you select. Each log type and content type have a default filter configuration that you can use as-is or modify. You can also create and save new filter configurations. These new filters can be based on the default filter or on an existing filter that you created previously. If you save the filter configuration, you can generate the same log view at a later date without having to configure the settings each time. You can delete your customized filter configurations if you no longer need them.

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.

Because logs contain some information that is collected at intervals, you can refresh your log views. To configure the log refresh rate, display the log and select from the **Auto-Refresh** list box at the top right on that log's view.

Note: If you view log data by using specific dates, the data stays the same when you click **Auto-Refresh**.

Reports and logs always display in the language that the management server was installed with. To display these 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.

See "What you can do from the logs" on page 626.

See "Saving and deleting custom logs by using filters" on page 628.

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.

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.

---

7   After you have the view configuration that you want, click **View Log**.

    The log view appears in the same window.

What you can do from the logs

Logs contain records about client configuration changes, security-related activities, and errors. These records are called events. The logs display these events with any relevant additional information. Security-related activities include information about virus detections, computer status, and the traffic that enters or exits the client computer.

Logs are an important method for tracking each client computer's activity and its interaction with other computers and networks. You can use this data to analyze the overall security status of the network and modify the protection on the client computers. You can track the trends that relate to viruses, security risks, and attacks. If several people use the same computer, you might be able to identify who introduces risks, and help that person to use better precautions.

You can view the log data on the **Logs** tab of the **Monitors** page.

The management server regularly uploads the information in the logs from the clients to the management server. You can view this information in the logs or in reports. Because reports are static and do not include as much detail as the logs, you might prefer to monitor the network by using logs.

Note: If you have only Symantec Network Access Control installed, only some of the logs contain data; some logs are empty. The Audit log, Compliance log, Computer Status log, and System log contain data. If you have only Symantec Endpoint Protection installed, the Compliance logs and Enforcer logs are empty but all other logs contain data.

In addition to using the logs to monitor your network, you can take the following actions from various logs:

- Run commands on client computers.
  See "Running commands from the computer status log" on page 630.

- Add several kinds of exceptions.
  See "Creating exceptions from log events in Symantec Endpoint Protection Manager" on page 541.

- Delete files from the **Quarantine**.
  See "Using the Risk log to delete quarantined files on your client computers" on page 367.

Table 25-3 describes the different types of content that you can view and the actions that you can take from each log.

Table 25-3   Log types

Log type	Contents and actions
Audit	The Audit log contains information about policy modification activity.
	Available information includes the event time and type; the policy modified; the domain, site, and user name involved; and a description.
	No actions are associated with this log.
Application and Device Control	The Application Control log and the Device Control log contain information about events where some type of behavior was blocked.
	The following Application and Device Control logs are available:
	■ Application Control, which includes information about Tamper Protection ■ Device Control
	Available information includes the time the event occurred, the action taken, and the domain and computer that were involved. It also includes the user that was involved, the severity, the rule that was involved, the caller process, and the target.
	You can create an application control or Tamper Protection exception from the Application Control log.
	See "Specifying how Symantec Endpoint Protection handles monitored applications" on page 537.
Compliance	The compliance logs contain information about the Enforcer server, Enforcer clients, and Enforcer traffic, and about host compliance.
	No actions are associated with these logs.
Computer Status	The Computer Status log contains information about the real-time operational status of the client computers in the network.
	Available information includes the computer name, IP address, infected status, protection technologies, Auto-Protect status, versions, and definitions date. It also includes the user, last check-in time, policy, group, domain, and restart required status.
	You can also clear the infected status of computers from this log.
	Note: This log contains information that is collected from both Windows clients and Mac clients.

<div style="text-align:center">

Table 25-3   Log types *(continued)*

</div>

Log type	Contents and actions
Network Threat Protection	The Network Threat Protection logs contain information about attacks on the firewall and on intrusion prevention. Information is available about denial-of-service attacks, port scans, and the changes that were made to executable files. They also contain information about the connections that are made through the firewall (traffic), and the data packets that pass through. These logs also contain some of the operational changes that are made to computers, such as detecting network applications, and configuring software.
	No actions are associated with these logs.
SONAR	The SONAR log contains information about the threats that have been detected during SONAR threat scanning. These are real-time scans that detect potentially malicious applications when they run on your client computers.
	The information includes items such as the time of occurrence, event actual action, user name, Web domain, application, application type, file, and path.
	If you have legacy clients in your network, the SONAR log can also contain information from legacy TruScan proactive threat scans.
	See "About SONAR" on page 395.
Risk	The Risk log contains information about risk events. Available information includes the event time, event actual action, user name, computer, and domain, risk name and source, count, and file and path.
Scan	The Scan log contains information about virus and spyware scan activity from both Windows clients and Mac clients.
	Available information includes items such as the scan start, computer, IP address, status, duration, detections, scanned, omitted, and domain.
	No actions are associated with these logs.
System	The system logs contain information about events such as when services start and stop.
	No actions are associated with these logs.

Saving and deleting custom logs by using filters

You can construct custom filters by using the **Basic Settings** and **Advanced Settings** to change the information that you want to see. You can save your filter settings to the database so that you can generate the same view again in the future. When you save your settings, they are saved in the database. The name you give

to the filter appears in the **Use a saved filter** list box for that type of logs and reports.

Note: If you selected **Past 24 hours** as the time range for a log filter, the 24-hour time range begins when you first select the filter. If you refresh the page, the start of the 24-hour range does not reset. If you select the filter, and wait to view a log, the time range starts when you select the filter. It does not start when you view the log.

If you want to make sure the past 24-hour range starts now, select a different time range and then reselect **Past 24 hours**.

To save a custom log by using a filter

1 In the main window, click **Monitors**.

2 On the **Logs** tab, select the type of log view that you want to configure a filter for from the **Log type** list box.

3 For some types of logs, a **Log content** list box appears. If it appears, select the log content that you want to configure a filter for.

4 In the **Use a saved filter** list box, select the filter that you want to start from. For example, select the default filter.

5 Under **What filter settings would you like to use**, click **Advanced Settings**.

6 Change any of the settings.

7 Click **Save Filter**.

8 In the dialog box that appears, in the **Filter name** box, type the name that you want to use for this log filter configuration. Only the first 32 characters of the name that you give display when the saved filter is added to the filter list.

9 Click **OK** and your new filter name is added to the **Use a saved filter** list box.

10 When the confirmation dialog box appears, click **OK**.

To delete a saved filter

1 In the **Use a saved filter** list box, select the name of the log filter that you want to delete.

2 Beside the **Use a saved filter** list box, click the **Delete** icon.

3 When you are prompted to confirm that you want to delete the filter, click **Yes**.

Viewing logs from other sites

If you want to view the logs from another site, you must log on to a server at the remote site from the Symantec Endpoint Protection Manager console. If you have an account on a server at the remote site, you can log on remotely and view that site's logs.

If you have configured replication partners, you can choose to have all the logs from the replication partners copied to the local partner and vice versa.

See "Specifying which data to replicate" on page 196.

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 from the computer status log

From the **Computer Status** log, you can take the following kinds of actions on client computers:

■ Run scans or cancel scans.

■ Restart the computers.

■ Update content.

■ Enable or disable several of the protection technologies.

You can also right-click a group directly from the **Clients** page of the Symantec Endpoint Protection Manager console to run commands.

See "About commands that you can run on client computers" on page 231.

See "Running commands on the client computer from the console" on page 233.

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. If you confirm the command, the table refreshes and you see that the cancel command is added to the command status table.

Note: If you run a scan command, and select a **Custom** scan, the scan uses the command scan settings that you configured on the **Administrator-defined Scans** page. The command uses the settings that are in the Virus and Spyware Protection policy that is applied to the selected client computers.

If you run a **Restart Client Computer** command from a log, the command is sent immediately. Users that are logged on to the client are warned about the restart based on the options that the administrator has configured for that client.

You can configure client restart options on the **General Settings** tab.

See "Restarting client computers" on page 145.

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**.

Managing notifications

This chapter includes the following topics:

- Managing notifications
- Establishing communication between the management server and email servers
- Viewing and acknowledging notifications
- Saving and deleting administrative notification filters
- Setting up administrator notifications
- How upgrades from another version affect notification conditions

Managing notifications

Notifications alert administrators and computer users about potential security problems.

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. After a few days, you can adjust the notifications settings.

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

Table 26-1 lists the tasks you can perform to manage notifications.

Table 26-1   Notification management

Task	Description
Learn about notifications	Learn how notifications work.
	See "How notifications work" on page 634.
Confirm that the email server is configured to enable email notifications	Notifications sent by email require that the Symantec Endpoint Protection Manager and the email server are properly configured.
	See "Establishing communication between the management server and email servers" on page 640.
Review preconfigured notifications	Review the preconfigured notifications provided by Symantec Endpoint Protection.
View unacknowledged notifications	View and respond to unacknowledged notifications.
	See "Viewing and acknowledging notifications" on page 640.
Configure new notifications	Optionally create notifications to remind you and other administrators about important issues.
	See "Setting up administrator notifications" on page 642.
	See "About turning on notifications for remote clients" on page 262.
Create notification filters	Optionally create filters to expand or limit your view of all of the notifications that have been triggered.
	See "Saving and deleting administrative notification filters" on page 641.

How notifications work

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

Events trigger a notification. A new security risk, a hardware change to a client computer, or a trialware license expiration can trigger a notification. Actions can then be taken by the system once a notification is triggered. An action might record the notification in a log, or run a batch file or an executable file, or send an email.

Note: Email notifications require that communications between the Symantec Endpoint Protection Manager and the email server are properly configured.

You can set a damper period for notifications. The damper period specifies the time that must pass before the notification condition is checked for new data. When a notification condition has a damper period, the notification is only issued on the first occurrence of the trigger condition within that period. For example, suppose a large-scale virus attack occurs, and that there is a notification condition configured to send an email whenever viruses infect five computers on the network. If you set a one hour damper period for that notification condition, the server sends only one notification email each hour during the attack.

See "Managing notifications" on page 633.

See "Establishing communication between the management server and email servers" on page 640.

See "What are the types of notifications and when are they sent?" on page 635.

See "Setting up administrator notifications" on page 642.

See "Viewing and acknowledging notifications" on page 640.

What are the types of notifications and when are they sent?

Symantec Endpoint Protection Manager provides notifications for administrators. You can customize most of these notifications to meet your particular needs. For example, you can add filters to limit a trigger condition only to specific computers. Or you can set notifications to take specific actions when they are triggered.

By default, some of these notifications are enabled when you install Symantec Endpoint Protection Manager. Notifications that are enabled by default are configured to log to the server and send email to system administrators.

See "Managing notifications" on page 633.

See "How upgrades from another version affect notification conditions" on page 643.

Table 26-2   Preconfigured notifications

Notification	Description
Authentication failure	A configurable number of logon failures in a defined period of time triggers the Authentication failure notification. You can set the number of logon failures and the time period within which they must occur to trigger the notification.

Table 26-2   Preconfigured notifications *(continued)*

Notification	Description
Client list changed	This notification triggers when there is a change to the existing client list. This notification condition is enabled by default.
	Client list changes can include:
	■ The addition of a client
	■ A change in the group of a client
	■ A change in the name of a client
	■ The deletion of a client
	■ A change in the hardware of a client
	■ A change in the Unmanaged Detector status of a client
	■ A client mode change
	This notification is enabled by default.
Client security alert	This notification triggers upon any of the following security events:
	■ Compliance events
	■ Network Threat Protection events
	■ Traffic events
	■ Packet events
	■ Device control events
	■ Application control events
	You can modify this notification to specify the type, severity, and frequency of events that determine when these notifications are triggered.
	Some of these occurrence types require that you also enable logging in the associated policy.
Download Protection content out-of-date	Alerts the administrators about out-of-date Download Protection content. You can specify the age at which the definitions trigger the notification.
Enforcer is down	This notification triggers when the Enforcer appliance goes offline. The notification tells you the name of each Enforcer, its group, and the time of its last status.
Forced application detected	This notification triggers when an application on the commercial application list is detected or when an application on the list of applications that the administrator monitors is detected.

Table 26-2 Preconfigured notifications *(continued)*

Notification	Description
IPS signature out-of-date	Alerts the administrators about out-of-date IPS signatures. You can specify the age at which the definitions trigger the notification.
Licensing issue **Paid license expiration**	This notification alerts administrators and, optionally, partners, about the paid licenses that have expired or that are about to expire. This notification is enabled by default.
Licensing issue **Over-deployment**	This notification alerts administrators and, optionally, partners, about over-deployed paid licenses. This notification is enabled by default.
Licensing issue **Trial license expiration**	This notification alerts administrators about expired trial licenses and the trial licenses that are due to expire in 60, 30, and 7 days. This notification is enabled by default if there is a trial license. It is not enabled by default if your license is due for an upgrade or has been paid. This notification is enabled by default.
New learned application	This notification triggers when application learning detects a new application.
New risk detected	This notification triggers whenever virus and spyware scans detect a new risk.
New software package	This notification triggers when a new software package downloads or the following occurs: ■ LiveUpdate downloads a client package. ■ The management server is upgraded. ■ The console manually imports client packages. You can specify whether the notification is triggered only by new security definitions, only by new client packages, or by both. By default, the **Client package** setting option is enabled and the **Security definitions** option is disabled for this condition. The **New client software** notification is enabled by default.

Table 26-2   Preconfigured notifications *(continued)*

Notification	Description
New user-allowed download	This notification triggers when a client computer allows an application that Download Insight detected. An administrator can use this information to help evaluate whether to block or allow the application.
Risk outbreak	This notification alerts administrators about security risk outbreaks. You set the number and type of occurrences of new risks and the time period within which they must occur to trigger the notification. Types of occurrences include occurrences on any computer, occurrences on a single computer, or occurrences on distinct computers.

This notification condition is enabled by default. |
| **Security Virtual Appliance offline** | This notification alerts administrators when a Security Virtual Appliance goes offline. Security Virtual Appliances run only in VMware vShield infrastructures. |
| **Server health** | Server health issues trigger the notification. The notification lists the server name, the health status, the reason, and the last online or offline status.

This notification is enabled by default. |
| **Single risk event** | This notification triggers upon the detection of a single risk event and provides details about the risk. The details include the user and the computer involved, and the actions that the management server took. |
| **SONAR definition out-of-date** | Alerts the administrators about out-of-date SONAR definitions. You can specify the age at which the definitions trigger the notification. |
| **System event** | This notification triggers upon certain system events and provides the number of such events that were detected.

System events include the following events:
- Server activities
- Enforcer activities
- Replication failures
- System errors |

Table 26-2   Preconfigured notifications *(continued)*

Notification	Description
Unmanaged computers	This notification triggers when the management server detects unmanaged computers on the network. The notification provides details including the IP address, the MAC address, and the operating system of each unmanaged computer.
Upgrade license expiration	Upgrades from previous versions of Symantec Endpoint Protection Manager to the current version are granted an upgrade license. This notification triggers when the upgrade license is due to expire. **Note:** The **Upgrade license expiration** notification appears only after a Symantec Endpoint Protection upgrade.
Virus definitions out-of-date	Alerts the administrators about out-of-date virus definitions. You can specify the age at which the definitions trigger the notification. This notification is enabled by default.

About partner notifications

When the management server detects that clients have paid licenses that are about to expire or that have expired, it can send a notification to the system administrator. Similarly, the management server can send a notification to the administrator when it detects that licenses are over-deployed.

However, in both of these cases, the resolution of the problem may require the purchase of new licenses or renewals. In many installations the server administrator may not have the authority to make such purchases, but instead relies upon a Symantec partner to perform this task.

The management server provides the ability to maintain the contact information for the partner. This information can be supplied when the server is installed. The system administrator can also supply or edit the partner information at any time after the installation in the Licenses pane of the console.

When the partner contact information is available to the management server, paid license-related notifications and over-deployed license notifications are sent automatically both to the administrator and to the partner.

See

Establishing communication between the management server and email servers

For the management server to send automatic email notifications, you must configure the connection between the management server and the email server.

See "Managing notifications" on page 633.

To establish communication between the management server and email servers

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

2   Under **Servers**, select the management server for which you want to establish a connection to the email server.

3   Under **Tasks**, click **Edit the server properties**.

4   In the **Server Properties** dialog box, click the **Email Server** tab.

5   Enter the email server settings.

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

6   Click **OK**.

Viewing and acknowledging notifications

You can view unacknowledged notifications or all notifications. You can acknowledge an unacknowledged notification. You can view all the notification conditions that are currently configured in the console.

The **Security Status** pane on the **Home** page indicates the number of unacknowledged notifications that have occurred during the last 24 hours.

See "Managing notifications" on page 633.

To view recent unacknowledged notifications

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

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

     A list of recent unacknowledged notifications appears under the **Notifications** tab.

3   Optionally, in the list of notifications, in the **Report** column, click the document icon if it exists.

     The notification report appears in a separate browser window. If there is no document icon, all of the notification information appears in the **Message** column in the list of notifications.

To view all notifications

1   In the console, click **Monitors** and then click the **Notifications** tab.

2   Optionally, on the **Notifications** tab, from the **Use a saved filter** menu, select a saved filter.

       See "Saving and deleting administrative notification filters" on page 641.

3   Optionally, on the **Notifications** tab, from the **Time range** menu, select a time range.

4   On the **Notifications** tab, click **View Notifications**.

To acknowledge a notification

1   View notifications.

       See "To view recent unacknowledged notifications" on page 640.

       See "To view all notifications" on page 641.

2   On the **Notifications** tab, in the list of notifications, in the **Ack** column, click the red icon to acknowledge the notification.

To view all configured notification conditions

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

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

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

Saving and deleting administrative notification filters

You can use filters to expand or limit your view of administrative notifications in the console. You can save new filters and you can delete previously saved filters.

See "Viewing and acknowledging notifications" on page 640.

See "Managing notifications" on page 633.

You can create a saved filter that uses any combination of the following criteria:

- **Time range**
- **Acknowledged status**
- **Notification type**
- **Created by**
- **Notification name**

For example, you can create a filter that only displays unacknowledged risk outbreak notifications posted during the past 24 hours.

To add a notification filter

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

2   On the **Monitors** page, on the **Notifications** tab, click **Advanced Settings**.

3   Under the **What filter settings would you like to use?** heading, set the criteria for the filter.

4   Click **Save Filter**.

5   On the **Notifications** tab, in the **Filter name** box, type a filter name, and then click **OK**.

To delete a saved notification filter

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

2   On the **Monitors** page, on the **Notifications** tab, on the **Use a saved filter** menu, choose a filter.

3   At the right of the **Use a saved filter** menu, click the **X** icon.

4   In the **Delete Filter** dialog box, click **Yes**.

Setting up administrator notifications

You can configure notifications to alert you and other administrators when particular kinds of events occur. You can also add the conditions that trigger notifications to remind you to perform important tasks. For example, you can add a notification condition to inform you when a license has expired, or when a security risk has been detected.

When triggered, a notification can perform specific actions, such as the following:

■   Log the notification to the database.

■   Send an email to one or more individuals.

■   Run a batch file.

Note: To send email notifications, you must configure an email server to communicate with the management server.

See "Establishing communication between the management server and email servers" on page 640.

You choose the notification condition from a list of available notification types.

Once you choose the notification type, you then configure it as follows:

■ Specify filters.
Not all notification types provide filters. When they do, you can use the filters to limit the conditions that trigger the notification. For example, you can restrict a notification to trigger only when computers in a specific group are affected.

■ Specify settings.
All notification types provide settings, but the specific settings vary from type to type. For example, a risk notification may allow you to specify what type of scan triggers the notification.

■ Specify actions.
All notification types provide actions you can specify.

To set up an administrator notification

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

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

3   On the **Notifications** tab, click **Add**, and then click a notification type.

4   In the **Add Notification Condition** dialog box, provide the following information:

■ In the **Notification name** text box, type a name to label the notification condition.

■ In the **What filter settings would you like to use?** area, if it is present, specify the filter settings for the notification condition.

■ In the **What settings would you like for this notification?** area, specify the conditions that trigger the notification.

■ In the **What should happen when this notification is triggered?** area, specify the actions that are taken when the notification is triggered.

5   Click **OK**.

See "Managing notifications" on page 633.

See "Viewing and acknowledging notifications" on page 640.

How upgrades from another version affect notification conditions

When Symantec Endpoint Protection is installed on a new server, many of the preconfigured notification conditions are enabled by default. An upgrade to

Symantec Endpoint Protection from a previous version, however, can affect which notification conditions are enabled by default. It can also affect their default settings.

The following notification conditions are enabled by default in a new installation of Symantec Endpoint Protection:

- **Client list changed**

- **New client software**

- **Over deployment issue**

- **Paid license issue**

- **Risk outbreak**

- **Server health**

- **Trialware license expiration**

- **Virus definitions out-of-date**

When an administrator upgrades the software from a previous version, all existing notification conditions from the previous version are preserved. However, existing **New software package** notification conditions become **New client software** notification conditions. The **New client software** condition has two settings that are not present in the **New software package** condition: **Client package** and **Security definitions**. When the software is upgraded, both of these settings are enabled for notification conditions of this type that are preserved across the upgrade. **New client software** notifications that are conditions created after the upgrade, however, have the **Client package** setting enabled and the **Security definitions** setting disabled by default.

Note: When the **Security definitions** setting in the **New client software** notification condition is enabled, it may cause a large number of notifications to be sent. This situation can occur when there are many clients or when there are frequently scheduled security definition updates. If you do not want to receive frequent notifications about security definition updates, you can edit the notification condition to disable the **Security definitions** setting

---

Several notification conditions may have a new setting that did not appear in earlier versions: **Send email to system administrators**. If that setting is new for a notification condition, it is disabled by default for any existing condition of that type following the upgrade.

When a default notification condition type has not been added in a previous installation, that notification condition is added in the upgraded installation.

However, the upgrade process cannot determine which default notification conditions may have been deleted deliberately by the administrator in the previous installation. With one exception, therefore, all of the following action settings are disabled in each default notification condition in an upgraded installation: **Send email to system administrators**, **Log the notification**, **Run batch file**, and **Send email to**. When all four of these actions are disabled, the notification condition is not processed, even though the condition itself is present. Administrators can edit the notification conditions to enable any or all of these settings.

Note that the **New client software** notification condition is an exception: it can produce notifications by default when it is added during the upgrade process. Unlike the other default notification conditions, both the **Log the notification** and the **Send email to system administrators** action settings are enabled for this condition.

If the previous version of the software does not support licenses, an **Upgrade license expiration** notification condition is enabled.

Some notification condition types are not available in previous versions of the software. Those notification conditions are enabled by default when the software is upgraded.

See "What are the types of notifications and when are they sent?" on page 635.

Section 4

Managing protection in virtual environments

Overview of Symantec Endpoint Protection and virtual infrastructures

This chapter includes the following topics:

- Using Symantec Endpoint Protection in virtual infrastructures

- About Shared Insight Cache

- About the Virtual Image Exception tool

Using Symantec Endpoint Protection in virtual infrastructures

Symantec Endpoint Protection provides the Shared Insight Cache and Virtual Image Exception features for virtual infrastructures, which you can enable to improve performance. You need to perform some additional installation and configuration tasks to enable these features.

Table 27-1   Virtual infrastructure features and their use

Feature and use	Description
Use a Shared Insight Cache to skip the scanning of files that are known to be clean.	Shared Insight Cache keeps track of the files that are known to be clean. Shared Insight Cache can reduce the scan load by eliminating the need to rescan those files.
	You can set up the following types of Shared Insight Cache:
	■ A vShield-enabled Shared Insight Cache Virtual clients in a VMware vShield infrastructure can use a vShield-enabled Shared Insight Cache reduce scan loads. ■ A network-based Shared Insight Cache Virtual clients that use any kind of virtual infrastructure can use a network-based Shared Insight Cache reduce scan loads.
	Note: Symantec supports the use of the vShield-enabled Shared Insight Cache only for VMware infrastructures.
	See "About Shared Insight Cache " on page 651.
	See "What do I need to do to use a vShield-enabled Shared Insight Cache?" on page 668.
	See "What do I need to do to use a network-based Shared Insight Cache?" on page 653.
Use the Virtual Image Exception tool so that clients can skip the scanning of base image files.	The Virtual Image Exception tool lets you mark base image files as safe so that scans skip those files to reduce scan loads.
	Note: Symantec does not support the use of the Virtual Image Exception tool in a physical environment.
	See "About the Virtual Image Exception tool" on page 651.
Configure the non-persistent virtual desktop infrastructures feature.	Symantec Endpoint Protection clients have a configuration setting to indicate that they are non-persistent virtual clients. You can configure a separate aging period for the offline GVMs in non-persistent virtual desktop infrastructures. Symantec Endpoint Protection Manager removes non-persistent GVM clients that have been offline longer than the specified time period.
	See "Configuring a separate purge interval for offline non-persistent VDI clients" on page 691.

The protection technologies in Symantec Endpoint Protection Manager and Symantec Endpoint Protection typically function the same way in virtual infrastructures as they do in physical infrastructures. You can install, configure, and use Symantec Endpoint Protection Manager and Symantec Endpoint Protection clients in virtual infrastructures in the same way as in physical infrastructures.

About Shared Insight Cache

Shared Insight Cache use improves performance in virtual infrastructures. Files that Symantec Endpoint Protection clients have determined to be clean are added to the cache. The subsequent scans that use the same virus definitions version can ignore the files that are in the Shared Insight Cache. Shared Insight Cache is used only for scheduled and manual scans.

The network-based Shared Insight Cache runs as a Web service that is independent of the Symantec Endpoint Protection client. Shared Insight Cache uses a voting system. After a client uses the latest content to scan a file and determines that it is clean, the client submits a vote to the cache. If the file is not clean, the client does not submit a vote. When the vote count for a file is greater than or equal to the vote count threshold, then Shared Insight Cache considers the file clean. When another client subsequently needs to scan the same file, that client first queries Shared Insight Cache. If the file is marked clean for their current content, then the client does not scan that file.

When a client sends a vote to Shared Insight Cache, the cache checks the version of content that the client used to scan the file. If the client does not have the latest content, Shared Insight Cache ignores the vote. If newer content is available, the newer content becomes the latest known content and Shared Insight sets the vote count back to one.

To keep the cache size manageable, Shared Insight Cache uses a pruning algorithm. The algorithm removes the oldest cache entries, which are those with the oldest timestamp, first. This algorithm ensures that the cache size does not exceed the memory usage threshold.

See "What do I need to do to use a network-based Shared Insight Cache?" on page 653.

See "What do I need to do to install a Security Virtual Appliance?" on page 669.

See "What do I need to do to use a vShield-enabled Shared Insight Cache?" on page 668.

See "Using Symantec Endpoint Protection in virtual infrastructures" on page 649.

About the Virtual Image Exception tool

The Virtual Image Exception tool lets clients bypass the scanning of the base image files for threats. This feature reduces the resource load on disk I/O and on the CPU.

Symantec Endpoint Protection supports the use of Virtual Image Exceptions for both managed clients and unmanaged clients.

Note: Symantec does not support the use of the Virtual Image Exception tool in physical environments.

See "Using the Virtual Image Exception tool on a base image" on page 685.

See "Using Symantec Endpoint Protection in virtual infrastructures" on page 649.

Installing and using a network-based Shared Insight Cache

This chapter includes the following topics:

What do I need to do to use a network-based Shared Insight Cache?

You can use a network-based Shared Insight Cache to improve scan performance.

Table 28-1   Tasks to install and use a network-based Shared Insight Cache

Step	Task
Step 1	Install Shared Insight Cache. See "System requirements for implementing a network-based Shared Insight Cache" on page 654. See "Installing and uninstalling a network-based Shared Insight Cache" on page 655.
Step 2	In the Virus and Spyware policy in Symantec Endpoint Protection Manager, enable your virtual clients to use Shared Insight Cache. See "Enabling or disabling the use of a network-based Shared Insight Cache" on page 656.

After you have installed a Shared Insight Cache, you can optionally do the following tasks:

■ Customize any of the service, cache, or log settings for Shared Insight Cache.
See "Customizing network-based Shared Insight Cache configuration settings" on page 658.

■ View related events in the log.
See "Viewing network-based Shared Insight Cache log events" on page 662.

■ Use the Windows Performance Manager to monitor its performance.
See "Monitoring network-based Shared Insight Cache performance counters" on page 664.

System requirements for implementing a network-based Shared Insight Cache

Table 28-2 describes the minimum system requirements that a virtual infrastructure needs to run Shared Insight Cache.

Table 28-2   Network-based Shared Insight Cache system requirements

Requirement	Description
Software	■ Windows Server 2003/2008 ■ .NET Framework 4
CPU	Shared Insight Cache must be installed on a dedicated server or a virtual machine.

Table 28-2   Network-based Shared Insight Cache system requirements
                    (continued)

Requirement	Description
Memory	2 GB minimum
Available disk space	100 MB minimum

See "About Shared Insight Cache " on page 651.

See "Installing and uninstalling a network-based Shared Insight Cache" on page 655.

Installing and uninstalling a network-based Shared Insight Cache

Before you install Shared Insight Cache, ensure that you have met all the system requirements and that you are logged on as a Windows administrator.

See "System requirements for implementing a network-based Shared Insight Cache" on page 654.

Note:

To install a network-based Shared Insight Cache

1   On the Symantec Endpoint Protection Tools product disc, navigate to the `Virtualization/SharedInsightCache` folder.

2   Double-click the following file to launch the installation program:

    `SharedInsightCacheInstallation.msi`

    Note: You can type the following command instead, to launch the same installation program:

    `msiexec /i SharedInsightCacheInstallation.msi`

3   In the **Shared Insight Cache Setup** wizard pane, click **Next**.

4   Read through the Symantec Software license agreement, check **I accept the terms of the License Agreement**, and then click **Next**.

5   On the **Destination Folder** pane, do one of the following tasks:

- Click **Next** to accept the default location for Shared Insight Cache.

- Click **Change**, browse to and select a different destination folder, click **OK**, and then click **Next**.

6 On the **Shared Insight Cache Settings** pane, specify the following Shared Insight Cache settings:

Cache Usage (% of Physical Memory)	The maximum size of the cache.
	When the cache exceeds this threshold, Shared Insight Cache prunes the cache size.
Listening Port	The port on which the server listens.
Status Listening Port	The port that the server uses to communicate status within the system.

7 Click **Install**.

8 When the installation has completed, click **Finish**.

See "Customizing network-based Shared Insight Cache configuration settings" on page 658.

Uninstalling Shared Insight Cache has the same effect as stopping the Shared Insight Cache service. If you are uncertain as to whether you want to permanently uninstall Shared Insight Cache, you can stop the service instead.

See "About stopping and starting the network-based Shared Insight Cache service" on page 662.

Note: To uninstall the Shared Insight Cache, use the appropriate Windows control panel, such as Add or Remove Programs. You must have Windows administrator rights to uninstall Shared Insight Cache.

If you uninstall Shared Insight Cache, you may also want to disable the Shared Insight Cache in Symantec Endpoint Protection Manager. Disabling Shared Insight Cache prevents the Windows Event log from receiving notifications each time clients cannot contact the cache.

Enabling or disabling the use of a network-based Shared Insight Cache

For communication over the network, by default Shared Insight Cache uses no authentication and no SSL. The default setting for the password is null. In other

words, the password is blank. If you change Shared Insight Cache settings to Basic authentication with SSL or Basic authentication with no SSL, you must specify a user name and password that can access Shared Insight Cache.

You can also change a user-defined authentication password. But if you do, you must specify that authentication user name and password in Symantec Endpoint Protection Manager so that clients can communicate with Shared Insight Cache.

To enable the use of a network-based Shared Insight Cache

1   In the Symantec Endpoint Protection Manager console, open the appropriate Virus and Spyware Protection policy and click **Miscellaneous**.

2   Click the **Shared Insight Cache** tab.

3   Check **Enable Shared Insight Cache**.

4   Click **Shared Insight Cache using the network**.

5   If you enabled SSL as a part of the Shared Insight Cache server settings in the configuration file, then click **Require SSL**.

    If you enable SSL, you must also set up your clients to communicate with Shared Insight Cache by adding the Shared Insight Cache server certificate to the trusted certificates authorities store for the local computer. Otherwise, the communication between the clients and the Shared Insight Cache fails.

    For information about how to add a server certificate, see your Active Directory documentation.

6   In the **Hostname** box, type the host name of the host on which you installed Shared Insight Cache.

7   In the **Port** box, type the port number of Shared Insight Cache.

8   Optionally, if you configured authentication for Shared Insight Cache, in the **Username** box, type the user name.

9   Optionally, if you configured authentication for Shared Insight Cache, click **Change Password** to change the default password (null) to the password that you created for authentication.

10 In the **New password** and the **Confirm password** boxes, type the new password.

    Leave these fields empty if you do not want to use a password.

11 Click **OK**.

See "What do I need to do to use a network-based Shared Insight Cache?" on page 653.

To disable the use of a network-based Shared Insight Cache

1   In the Symantec Endpoint Protection Manager console, open the appropriate
     Virus and Spyware Protection policy and click **Miscellaneous**.

2   Click the **Shared Insight Cache** tab.

3   Uncheck **Enable Shared Insight Cache**.

4   Click **OK**.

Customizing network-based Shared Insight Cache configuration settings

After you install Shared Insight Cache, you can customize its settings in the
configuration file.

The configuration file is an XML file that follows .NET Framework application
configuration standards. Shared Insight Cache does not start if there is an invalid
configuration, such as invalid XML, incorrect value types, or missing required
values.

For more information, click the following link:

Configuration Editor Tool (SvcConfigEditor.exe)

Table 28-3 describes the options that you can configure.

Table 28-3   Shared Insight Cache configuration options

Option and default value	Description and comments
Cache Service Listening Port The default value is 9005.	Port on which the service listens. If the range is not between 0 - 65535, the service does not start. The service does not start if it cannot listen on the specified port. `<endpoint address="http://localhost:9005/1"` By default, the Shared Insight Cache server listens on all IP addresses. To configure the listening IP addresses for HTTP or HTTPS services, you must use HttpCfg.exe (Windows 2003) or Netsh.exe (Windows 2008). The Shared Insight Cache server listens on the IP addresses that you specified in the IP Listen List modified by those tools. Netsh.exe is included with Windows 2008. You can install HttpCfg.exe from the Windows 2003 installation disc. The installer is located at the following path: `\Support\Tools\Suptools.msi` For more information, click following link: Configuring HTTP and HTTPS
Status Service Listening Port The default value is 9006.	Port on which the service listens. The service does not start if the range is not between 0 - 65535. The service does not start if it cannot listen on the specified port.
Vote Count The default value is 1.	Number of the clients that must verify that the file is clean before Shared Insight Cache uses the results. The value must be less than or equal to 15. If the value is greater than 15, the server uses the default value. `<cache.configuration vote.count="1"`
Prune Size The default value is 10.	Percentage of memory usage to remove from the cache when the cache hits the memory usage limit. The value must be between 10 and 100. If the value is not between 10 and 100, the server uses the default value. **Note:** Symantec recommends that you keep the default prune size. `prune.size="10"`

Table 28-3   Shared Insight Cache configuration options *(continued)*

Option and default value	Description and comments
Memory Usage The default value is 50.	Percentage of size of the cache before Shared Insight Cache starts pruning the cache. Must be greater than or equal to 10. `mem.usage="50"`
Log File The default value is *install_folder/* CacheServer.log	A file for the Shared Insight Cache log. `<filevalue="CacheServer.log" />`
Log Level The default value is ERROR.	ALL DEBUG INFO WARN ERROR FATAL OFF A value of OFF indicates that Shared Insight Cache does not log any messages. `<level value="ERROR" />` See "Viewing network-based Shared Insight Cache log events" on page 662.
Log Size The default value is 10000.	Size of the log (in bytes) until Shared Insight Cache rolls the log over. `<maximumFileSizevalue="10000" />`
Log Backups The default value is 1.	Number of rolled over logs to keep before the oldest log is deleted. A value of 0 indicates that Shared Insight Cache retains no backups. A negative value indicates that Shared Insight Cache retains an unlimited number of backups. `<maxSizeRollBackupsvalue="1" />`

Table 28-3 Shared Insight Cache configuration options *(continued)*

Option and default value	Description and comments

Enable SSL
 	
Enable authentication
	By default, Shared Insight Cache is set up with no authentication and no SSL. It can be changed to Basic authentication with SSL, no authentication with SSL, or Basic authentication with no SSL.
	
	``
	<webHttpBinding>
	<bindingname="CacheServerBinding">
	<!--
	       Uncomment the appropriate section to get
	       the desired security.
	
	       If enabling ssl modify the uri to use https.
	       A cert will also have to be installed and
	       registered for the ip/port.
	-->
	<!-- Basic authentication with SSL. >
	<security mode="Transport">
	<transport clientCredentialType="Basic"/>
	</security-->
	<!-- No authentication with SSL. >
	<security mode="Transport">
	<transport clientCredentialType="None"/>
	</security-->
	<!-- Basic authentication with no SSL. >
	<security mode="TransportCredentialOnly">
	<transport clientCredentialType="Basic"/>
	</security-->
	<!-- No authentication with no SSL. DEFAULT -->
	<securitymode="None">
	<transportclientCredentialType="Basic"/>
	</security>
	</binding>
	</webHttpBinding>
	``
	
	See "Enabling or disabling the use of a network-based Shared Insight Cache" on page 656.

To customize Shared Insight Cache settings

1   Navigate to and open the following file:

   Installation folder\SharedInsightCacheInstallation.exe.config

2   Make the modifications as needed.

3   Save your changes and close the file.

4   Restart the Shared Insight Cache service.

     You must restart the Shared Insight Cache service for changes to all
     configuration settings except the log level to take effect.

     See "About stopping and starting the network-based Shared Insight Cache
     service" on page 662.

See "What do I need to do to use a network-based Shared Insight Cache?"
on page 653.

About stopping and starting the network-based Shared Insight Cache service

You may need to stop the Shared Insight Cache service temporarily to troubleshoot
an issue. After you have resolved the issue, you can restart the service. You can
start and stop the service from the Service Control Manager.

Uninstalling Shared Insight Cache has the same effect as stopping the Shared
Insight Cache service. If you are uncertain as to whether you want to permanently
uninstall Shared Insight Cache, you can stop the service instead.

You must have Windows administrator rights to stop and start the Shared Insight
Cache service.

See "Troubleshooting issues with Shared Insight Cache " on page 665.

Viewing network-based Shared Insight Cache log events

You can view the Shared Insight Cache log file to see any events that Shared
Insight Cache creates. The log file is located in the installation folder and is named
`CacheServer.log`.

Shared Insight Cache prints logs in the following format:

```
[|] %thread | %d{MM/dd/yyyyHH:mm:ss} | %level | %logger{2} | %message [-]%newline
```

For example:

```
[|] 4 | 12/15/2010 10:51:37 | INFO | CacheServerService.Service | Started service [-]
```

Modify the configuration file to specify the log level that you want to use for
network-based Shared Insight Cache.

Table 28-4 describes the levels that you can set.

Table 28-4   Network-based Shared Insight Cache log levels

Log level	Description
OFF	OFF indicates that no incidents are logged.
FATAL	FATAL messages require you to take action. These messages are the errors that cause Shared Insight Cache to stop.
	For example, a FATAL message may indicate that the server IP address is not available, which means that Shared Insight Cache cannot run.
ERROR	ERROR messages require you to take action, but the process continues to run. They are errors in the system that cause Shared Insight Cache to fail or lose functionality.
	You also receive all log entries for FATAL messages.
	This level is the default logging level.
WARN	WARN messages indicate Shared Insight Cache behavior that may be undesirable, but do not cause it to fail.
	You also receive all log entries for FATAL messages and ERROR messages.
INFO	INFO messages describe the general actions of or give information about Shared Insight Cache. They may indicate the state of the system and help validate behavior or track down issues. However, alone they are not intended to report actionable items.
	For example, an information message may indicate that cache pruning is complete. The message does not detail a problem. It only logs behavior.
	You also receive all log entries for FATAL messages, ERROR messages, and WARN messages.
DEBUG ALL	DEBUG and ALL log level messages produce the same results. These log levels are intended for Support to troubleshoot problems with Shared Insight Cache.
	You also receive all log entries for all other log levels.

Increase the log level only when you need to troubleshoot issues with Shared Insight Cache. When you increase the log level, you begin to significantly increase the size of the log file. When you resolve the issue, return to the default log level of ERROR.

To view Shared Insight Cache events in the log

◆   Go to the following location:

    Installation folder/CacheServer.log

See "Customizing network-based Shared Insight Cache configuration settings" on page 658.

Monitoring network-based Shared Insight Cache performance counters

You can view network-based Shared Insight Cache statistics in the Windows Performance Monitor. The Shared Insight Cache service must be running to view its performance counters.

Table 28-5   Shared Insight Cache statistics

Statistic	Description
The number of items in the cache	This number represents the current number of items in the cache.
The number of items in the cache that have been voted clean	This number represents the current number of items in the cache, which have been voted clean.
Number of cache requests	The number of cache requests that have been made to the Shared Insight Cache service. This number includes only the number of valid requests that received a 200 response. This counter does not persist across restarts of the service.
Number of update requests	The number of update requests that have been made to the service. This number is only the valid requests that received a 200 response. This counter does not persist across restarts of the service.

To monitor network-based Shared Insight Cache performance counters

1   At the command prompt, type the following command:

     perfmon

2   In the **Performance** window, right-click the graph.

3   Select **Add Counters**.

4   In the **Performance object** drop-down list, select **Shared Insight Cache**.

5   Select the counters that you want to view, and click **Add**.

6   Click **Close**.

The Shared Insight Cache counters that you selected appear in the Performance graph.

For more information about using the Windows performance monitor, see your Windows documentation.

See "Troubleshooting issues with Shared Insight Cache " on page 665.

See "What do I need to do to use a network-based Shared Insight Cache?" on page 653.

Troubleshooting issues with Shared Insight Cache

Table 28-6 provides suggestions for how to troubleshoot issues with Shared Insight Cache.

Table 28-6   Troubleshooting Shared Insight Cache

Issue	Explanation/Resolution
Experiencing problems with the cache results	Restart the service. See "About stopping and starting the network-based Shared Insight Cache service" on page 662.
Shared Insight Cache returns a "no result" response	Shared Insight Cache returns a no result response when it fails to successfully perform a cache lookup. If the client requests a cache lookup, a no result means that the file must be scanned. **Note:** Shared Insight Cache returns a success response even when it fails to successfully perform a cache update. The reason is because the client is not required to perform a different action when a failure occurs.
Suspected issues with HTTP traffic	View the HTTP traffic error log. The HTTP traffic errors are logged in the following location: `%Windir%\System32\Logfiles\HTTPERR`

See "Viewing network-based Shared Insight Cache log events" on page 662.

See "Monitoring network-based Shared Insight Cache performance counters" on page 664.

Installing a Security Virtual Appliance and using a vShield-enabled Shared Insight Cache

This chapter includes the following topics:

- What do I need to do to use a vShield-enabled Shared Insight Cache?

- What do I need to do to install a Security Virtual Appliance?

- About the Symantec Endpoint Protection Security Virtual Appliance

- VMware software requirements to install a Symantec Security Virtual Appliance

- VMware software requirements for the Guest Virtual Machines

- Configuring the Symantec Endpoint Protection Security Virtual Appliance installation settings file

- Installing a Symantec Endpoint Protection Security Virtual Appliance

- Enabling Symantec Endpoint Protection clients to use a vShield-enabled Shared Insight Cache

- Stopping and starting the vShield-enabled Shared Insight Cache service

- Service commands for the vShield-enabled Shared Insight Cache

- Configuration file settings for a vShield-enabled Shared Insight Cache

- About vShield-enabled Shared Insight Cache event logging

■ Uninstalling a Symantec Endpoint Protection Security Virtual Appliance

What do I need to do to use a vShield-enabled Shared Insight Cache?

A vShield-enabled Shared Insight Cache runs in a Symantec Endpoint Protection Security Virtual Appliance. Windows-based Guest Virtual Machines (GVMs) use VMware vShield Endpoint to access the Shared Insight Cache.

Note: Symantec supports the use of a vShield-enabled Shared Insight Cache only in VMware ESX/ESXi infrastructures.

Table 29-1   Tasks that you need to perform to use a vShield-enabled Shared Insight Cache

Step	Task
Step 1	Install a Security Virtual Appliance on an ESX/ESXi host. See "What do I need to do to install a Security Virtual Appliance?" on page 669.
Step 2	Install the VMware EPSEC driver on each GVM so that they can communicate with the Security Virtual Appliance. See "VMware software requirements for the Guest Virtual Machines" on page 672.
Step 3	Enable the GVMs (clients) to use Shared Insight Cache. You perform this task from the Virus and Spyware Protection policy in the Symantec Endpoint Protection Manager. See "Enabling Symantec Endpoint Protection clients to use a vShield-enabled Shared Insight Cache" on page 678.

After you enable GVM clients to use a vShield-enabled Shared Insight Cache, you can optionally configure administrator notifications for Security Virtual Appliances that go offline.

See "Setting up administrator notifications" on page 642.

What do I need to do to install a Security Virtual Appliance?

A vShield-enabled Shared Insight Cache runs in a Symantec Endpoint Protection Security Virtual Appliance. You must install the appliance so that Windows-based Guest Virtual Machines (GVMs) can use VMware vShield Endpoint to access the Shared Insight Cache.

Note: Symantec supports the use of the Security Virtual Appliance only in VMware ESX/ESXi infrastructures.

Table 29-2 Tasks that you need to perform to install a Symantec Endpoint Protection Security Virtual Appliance

Step	Task
Step 1	Install and configure the prerequisite VMware software that you need. See "VMware software requirements to install a Symantec Security Virtual Appliance" on page 671. For information about how to install and configure VMware software, refer to your VMware documentation.
Step 2	In Symantec Endpoint Protection Manager, export the communication settings file from the client group that you plan to use for your Guest Virtual Machines (GVMs). You must have this file to install the Security Virtual Appliance. See "Exporting the client-server communications file manually" on page 702.
Step 3	Update the installation settings file with the information that the installation executable requires to install the Security Virtual Appliance on the ESXi host. See "Configuring the Symantec Endpoint Protection Security Virtual Appliance installation settings file" on page 672.
Step 4	Install the Security Virtual Appliance on the ESX/ESXi host. See "Installing a Symantec Endpoint Protection Security Virtual Appliance" on page 675.

After you install a Security Virtual Appliance, you can enable a vShield-enabled Shared Insight Cache for your GVMs to use.

See "What do I need to do to use a vShield-enabled Shared Insight Cache?" on page 668.

About the Symantec Endpoint Protection Security Virtual Appliance

The Symantec Endpoint Protection Security Virtual Appliance is a Linux-based virtual appliance that you install on a VMware ESX/ESXi server. The Security Virtual Appliance integrates with VMware's vShield Endpoint. The Shared Insight Cache runs in the appliance and lets Windows-based Guest Virtual Machines (GVMs) share scan results. Identical files are trusted and therefore skipped across all of the GVMs on the ESX/ESXi host. Shared Insight Cache improves full scan performance by reducing disk I/O and CPU usage.

Note: You must install a Security Virtual Appliance on each ESX/ESXi host if you want the GVMs to access Shared Insight Cache.

Figure 29-1   Symantec Endpoint Protection Security Virtual Appliance architecture
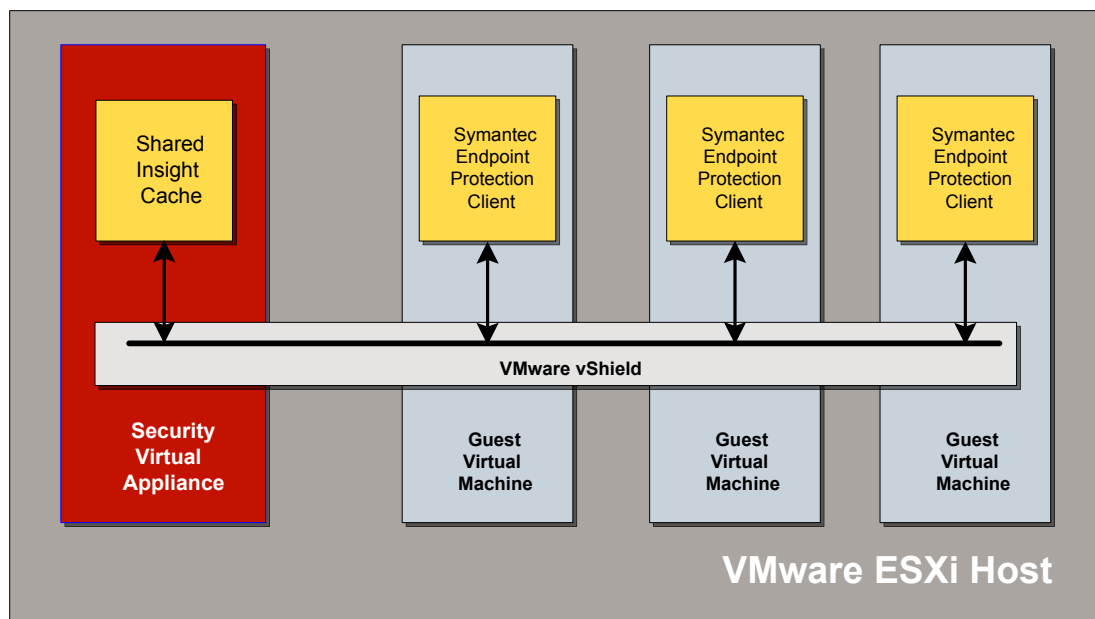
The appliance is complete and ready to use as soon as you install it. The appliance includes the Shared Insight Cache.

See "About Shared Insight Cache " on page 651.

See "VMware software requirements to install a Symantec Security Virtual Appliance" on page 671.

See "What do I need to do to install a Security Virtual Appliance?" on page 669.

VMware software requirements to install a Symantec Security Virtual Appliance

Table 29-3 describes the VMware components that you must have installed before you can install a Security Virtual Appliance. Once you have installed the appliance, you can enable a vShield-enabled Shared Insight Cache for the Guest Virtual Machines to use.

Table 29-3   VMware software requirements and prerequisites for installing a Security Virtual Appliance

Requirement	Description
VMware ESXi server software	One of the following versions: ■ ESX 4.1, with Patch ESX410-201107001 ■ ESXi 5.0 Update 1
VMware vShield product software	■ VMware vShield Manager 5.0 Update 1 ■ VMware vShield Endpoint 5.0 Update 1 **Note:** You must use vShield Manager 5.0 Update 1 to deploy vShield Endpoint 5.0 Update 1 to each host you want to manage. For more information about using VMware vShield Endpoint 5.0 Update 1, see the following Web page: Using vShield Endpoint 5.0 and vShield Data Security 5.0 with vSphere 4.1

Note: The Java Runtime Environment 7 or later is required to run the Security Virtual Appliance installation tool.

See "Installing a Symantec Endpoint Protection Security Virtual Appliance" on page 675.

See "What do I need to do to install a Security Virtual Appliance?" on page 669.

See "VMware software requirements for the Guest Virtual Machines" on page 672.

VMware software requirements for the Guest Virtual Machines

Table 29-4 describes the Guest Virtual Machines requirements to use the vShield-enabled Shared Insight Cache on the Symantec Security Virtual Appliance.

Table 29-4   VMware requirements for the Guest Virtual Machines

Requirement	Description
Guest Virtual Machines (GVMs)	The EPSEC 2.0 driver must be installed on all GVMs. On GVMs hosted by ESX 4.1 with Patch ESX410-201107001 applied, download the EPSEC driver locally and execute the installer on the virtual machine On GVMs hosted by ESXi 5.0 Update 1, do one of the following: ■ Download the EPSEC driver locally and execute the installer on the virtual machine or ■ Use the VMware Tools installer to install the EPSEC driver. **Note:** Perform a custom install and select vShield drivers under VMware device drivers/VMCI drivers, or perform a complete install.

See "What do I need to do to use a vShield-enabled Shared Insight Cache?" on page 668.

See "VMware software requirements to install a Symantec Security Virtual Appliance" on page 671.

Configuring the Symantec Endpoint Protection Security Virtual Appliance installation settings file

You must configure the SVA_InstallSettings.xml file before you can install the Security Virtual Appliance. This file is located in the Virtualization\SecurityVirtualAppliance folder of the Tools product disc.

Note: All settings are mandatory for installation unless explicitly marked as optional.

Table 29-5   Security Virtual Appliance installation file settings

Setting	Description
VMware vCenter information ■ IP address ■ User name ■ Password	Set the VMware vCenter IP address, user name, and password for the Security Virtual Appliance installation. ``` <vCenter> <ip_address>192.168.x.x</ip_address> <username>username</username> <!-- <password>password</password> --> </vCenter> ``` **Note:** vCenter Administrator user name and password are required to install the Security Virtual Appliance. If you do not configure the password in this settings file, then the installation prompts you for the password. Note that to install or uninstall the Security Virtual Appliance, the vCenter Administrator account that you use must have permissions in the following privilege categories: ■ Datastore (All privileges) ■ Network (All privileges) ■ vApp (All privileges) ■ Virtual Machine (All privileges) ■ Global > Cancel Task You cannot set these permissions from the Symantec Endpoint Protection Security Virtual Appliance installation settings file.
VMware vShield Manager information ■ IP address ■ User name ■ Password	Set the VMware vShield Manager IP address, user name, and password for the Security Virtual Appliance installation. **Note:** vShield Administrator credentials are required to install the Security Virtual Appliance. If you do not configure the password in this settings file, then the installation prompts you for the password. ``` <vShield> <ip_address>192.168.x.y</ip_address> <username>admin</username> <!-- <password>default</password> --> </vShield> ```

Table 29-5   Security Virtual Appliance installation file settings *(continued)*

Setting	Description

Installation settings
 	
■ Symantec Endpoint Protection Security Virtual Appliance OVA file location
■ ESXi host IP address
■ `sylink_xml` file location
■ Datastore prompt
	Provide the information that guides the Security Virtual Appliance installation.
	
	The installation package is the Symantec Endpoint Protection Security Virtual Appliance OVA file that you download from File Connect at https://fileconnect.symantec.com. To access File Connect, you need to have the activation serial number that is part of your license certificate available.
	
	The sylink.xml file contains the client group communication settings that you exported from the Symantec Endpoint Protection Manager.
	
	See "Exporting the client-server communications file manually" on page 702.
	
	You can change the datastore prompt to zero if you want to install automatically on the first datastore for the ESXi host.
	
	`<Installation>`
	    `<location_of_package>path to OVA file</location_of_package>`
	    `<esx_ip_address>192.168.x.z</esx_ip_address>`
	    `<sylink_xml>./sylink.xml</sylink_xml>`
	    `<datastore_prompt>1</datastore_prompt>`
	 `</Installation>`

Table 29-5	Security Virtual Appliance installation file settings *(continued)*

Setting	Description

Security Virtual Appliance information
 	
■ SVA host name
■ SVA admin password
■ SVA network settings (Optional)
    ■ IP address
    ■ Gateway
    ■ Subnet
    ■ DNS
	Set the Security Virtual Appliance host name. The host name must be unique within the vCenter. The host name is limited to alphanumeric characters and the hyphen character.
	
	The login account name for the Security Virtual Appliance is `admin`.
	
	Note: If you do not configure the admin account password in this settings file, then the installation prompts you for the password.
	
	Optionally, you can configure the Security Virtual Appliance network settings. By default the network settings are commented out and installation defaults to use DHCP. You are not required to use network settings to install a Security Virtual Appliance.
	
	Note: If you want to specify one of the Security Virtual Appliance network settings, you must uncomment and specify all four of them. If you specify only one to three of the network settings, the installation fails.
	
	`<sva>`
	
	`    <hostname>Symantec-SVA</hostname>`
	
	`    <admin_password>symantec</admin_password>`
	
	`<!--`
	`    <ip_address>192.168.x.w</ip_address>`
	`    <gateway>192.168.x.v</gateway>`
	`    <subnet>255.255.255.0</subnet>`
	`    <dns>192.168.x.u</dns>`
	`-->`
	`</sva>`

See "Installing a Symantec Endpoint Protection Security Virtual Appliance" on page 675.

See "What do I need to do to install a Security Virtual Appliance?" on page 669.

Installing a Symantec Endpoint Protection Security Virtual Appliance

After you have met the prerequisites, you can install the Security Virtual Appliance. You use the Security Virtual Appliance installation tool from the

command line. You must install a Security Virtual Appliance on each ESXi host if you want the GVMs on the host to use vShield-enabled Shared Insight Cache.

To install or uninstall the Security Virtual Appliance, the vCenter Administrator account that you use must have permissions in the following privilege categories:

- Datastore (All privileges)

- Network (All privileges)

- vApp (All privileges)

- Virtual Machine (All privileges)

- Global > Cancel Task

Note: As part of the installation process, the Security Virtual Appliance and its associated ESXi host registers with vShield Manager. For this reason, you should not use vMotion with the Security Virtual Appliance. A best practice is to use the sva_install.jar utility to uninstall and reinstall the Security Virtual Appliance.

See "VMware software requirements to install a Symantec Security Virtual Appliance" on page 671.

Note: The Java Runtime Environment 7 or later is required to run the Security Virtual Appliance installation tool.

To install a Security Virtual Appliance

1   On the Tools product disc, locate the
    `Virtualization\SecurityVirtualAppliance` folder.

2   Copy the entire contents of the `SecurityVirtualAppliance` folder to a local directory.

    For convenience, you may want to copy the files to the same location as the `sylink.xml` file that you exported from the Symantec Endpoint Protection Manager.

3   Configure the `SVA_InstallSettings.xml` file.

    The default name of the communications file that you exported from Symantec Endpoint Protection Manager is *group name*`_sylink.xml`. Be sure to change the `<sylink_xml>` pathname in the `SVA_InstallSettings.xml` file to match your exported file name.

    See "Configuring the Symantec Endpoint Protection Security Virtual Appliance installation settings file" on page 672.

4 Take a snapshot of the vShield Manager. During installation, the Security Virtual Appliance registers with the vShield Manager. A snapshot ensures that you can revert to the previous state, in case any Security Virtual Appliance installation issues occur.

5 At the command line, type the following command:

```
java -jar Symantec_SVA_Install.jar -s
pathname/SVA_InstallSettings.xml
```

By default, if there is more than one datastore available the installation prompts you to select one. If there is more than one network, the installation prompts you to select one.

Errors and other installation output are written to the `SVA_Install.log` file. This log file is created in the same directory where you executed the installation command.

Note: In a few instances, the write to that directory may fail. In these cases, the file is written to the /temp directory and is named SVA_Install*xxx*.log, where the system replaces xxx with a random number.

You can perform the following actions to recover from an incomplete Security Virtual Appliance installation or an aborted Security Virtual Appliance installation.

To recover from an incomplete installation or an aborted installation

1 Check to see if the Security Virtual Appliance is listed under the ESXi host.

2 If it is listed, turn off the Security Virtual Appliance and delete it from the disk.

3 Revert the vShield Manager to the snapshot that you took before you tried to install the Security Virtual Appliance.

4 Reinstall the Security Virtual Appliance.

Once you have installed a Security Virtual Appliance, you can log in with the admin account.

Enabling Symantec Endpoint Protection clients to use a vShield-enabled Shared Insight Cache

To enable clients to use a vShield-enabled Shared Insight Cache

1   In the Symantec Endpoint Protection Manager console, open the appropriate Virus and Spyware Protection policy and click **Miscellaneous**.

2   On the **Miscellaneous** page, click **Shared Insight Cache**.

3   Check **Enable Shared Insight Cache**.

4   Click **Shared Insight Cache using VMware vShield**.

5   Click **OK**.

See "What do I need to do to use a vShield-enabled Shared Insight Cache?" on page 668.

Stopping and starting the vShield-enabled Shared Insight Cache service

Once you have installed a Security Virtual Appliance, the Shared Insight Cache service starts automatically. If you want to change the settings in the Shared Insight Cache configuration file, you should stop the service before you edit the file.

To stop the vShield-enabled Shared Insight Cache service

1   Log in to the Security Virtual Appliance as admin with the password that you assigned in the installation settings file.

2   On the command line, type the following command:

```
sudo stop vsic
```

To start the vShield-enabled Shared Insight Cache service

1   Log in to the Security Virtual Appliance as admin with the password that you assigned in the installation settings file.

2   On the command line, type the following command:

```
sudo start vsic
```

See "Configuration file settings for a vShield-enabled Shared Insight Cache" on page 679.

Service commands for the vShield-enabled Shared Insight Cache

To issue service commands, you must log on to the Security Virtual Appliance using the admin account. The default password is **symantec**, but you were prompted to change the password the first time that you logged in.

Table 29-6 summarizes the commands that you can use.

Table 29-6 Service commands for the vShield-enabled Shared Insight Cache

Command	Description
sudo start vsic	Starts the vShield-enabled Shared Insight Cache service.
sudo stop vsic	Stops the vShield-enabled Shared Insight Cache service.
sudo restart vsic	If the vShield-enabled Shared Insight Cache service is running, stops the vShield-enabled Shared Insight Cache service and then starts it again.
sudo status vsic	Returns the status of the vShield-enabled Shared Insight Cache service.

See "Configuration file settings for a vShield-enabled Shared Insight Cache" on page 679.

See "Stopping and starting the vShield-enabled Shared Insight Cache service" on page 678.

Configuration file settings for a vShield-enabled Shared Insight Cache

The configuration file for a vShield-enabled Shared Insight Cache is an XML file that follows the .NET application configuration standard. The Shared Insight Cache service does not start if there is any invalid configuration, which includes invalid XML, incorrect value types, or missing required values.

The configuration file is named `SharedInsightCacheService.exe.config` and it is located in the `/etc/symantec` directory.

Note: Symantec has tested and optimized the default settings in this file for performance and scalability. Symantec recommends that you do not modify these settings. If you feel that you have a compelling reason to do so, we recommend that you contact Symantec Support first, before you make any changes.

Before you make any changes to the configuration file, create a backup copy of the file. You should also remember to restart the vShield-enabled Shared Insight Cache service after you have saved your changes.

Table 29-7 Configuration options

Option and default value	Description and comments
Cache prune size `prune.size="10"`	Percentage of memory usage to remove from the cache when the cache reaches the memory usage limit. The value must be between 10 and 100. If the value is not between 10 and 100, the server uses the default value of 10. **Note:** Avoid modifying this setting.
Cache memory usage `mem.usage="50"`	The maximum percentage of physical memory that the service is allowed to use. Once this value is reached, the service prunes the cache. This value must be 10 or greater.
Cache pruning interval `clean.interval="10"`	The interval in seconds at which the service checks to see if the cache should be pruned.
Enable performance statistics logging `enabled="true"`	Set to false to disable. **Note:** The `interval` attribute can override this setting.

Performance statistics log file
 	
`file="/data/Symantec/vSIC/`
`vSIC_Perf.csv"`
	The location of the file that collects performance data.

Performance statistics interval `interval="10"`	The interval, in seconds, at which statistics are recorded. If set to 0, this attribute disables recording and overrides the enabled=true attribute.
Performance statistics file maximum size `maxSize="1MB"`	The maximum size in bytes that the output file is allowed to reach before is rolled over to a backup file. You can also specify the maximum size in kilobytes, megabytes, or gigabytes. The value 10KB is interpreted as 10240 bytes.

Table 29-7   Configuration options *(continued)*

Option and default value	Description and comments
Number of performance statistics file backups maxBackups="1"	If set to zero, then there are no backup files and the log file is truncated when it reaches the maximum size (`maxSize` attribute). If this attribute is set to a negative number, then no deletions are made. **Note:** When you restart the service after you make a change to the `maxBackups` attribute, the existing backup files are overwritten. Symantec recommends that you move the existing backup files to a new location before you restart the service.

Table 29-8   Description of the logging configuration options

Option and default value	Description and comments
Log file file value="/data/log/Symantec/vSIC.log"	The file where the service logs information about the Security Virtual Appliance and vShield-enabled Shared Insight Cache.
Number of backup files to keep maxSizeRollBackups value="1"	If this attribute is set to zero, then there are no backup files and the log file is truncated when it reaches the value of the `maxSize` attribute. **Note:** When you restart the service after you make a change to the `maxBackups` attribute, the existing backup files are overwritten. Symantec recommends that you move the existing backup files to a new location before you restart the service.
Log size maximumFileSize value="10MB"	Size of the log (in bytes) before the oldest log is deleted.
Enable the local or remote logging option appender-ref ref="LocalSyslogAppender" appender-ref ref="RemoteSyslogAppender"	You can enable local or remote Syslog logging by uncommenting one of the options. Syslog is not enabled by default. If you want to log remotely, be sure to set the IP address for the `RemoteSyslogAppender`.
IP address for remote logging remoteAddress value="192.168.x.y"	You need to set this address if you enable remote logging.

Table 29-8   Description of the logging configuration options *(continued)*

Option and default value	Description and comments
Log level `level value="ERROR"`	ALL DEBUG INFO WARN ERROR FATAL OFF Each level includes the messages from the levels that are more critical as well. For example, ERROR logs the ERROR-level messages and the FATAL messages. The INFO level includes all messages except the debugging messages. **Note:** Set the value to OFF if you want to disable logging entirely.

See "Stopping and starting the vShield-enabled Shared Insight Cache service" on page 678.

For information about the .NET application configuration standard, see the following Web page:

Configuration Editor Tool (SvcConfigEditor.exe)

For more information about log4net configuration, see the following Web page:

Apache Logging Services

About vShield-enabled Shared Insight Cache event logging

Symantec Endpoint Protection logs the events from a Shared Insight Cache that is integrated with VMware vShield Endpoint to the `vSIC.log` file by default. This file is created in the `/data/log/Symantec` directory by default.

Logging is on by default and the level is set to `ERROR`. You can change the logging level and other logging attributes in the Shared Insight Cache configuration file.

See "Configuration file settings for a vShield-enabled Shared Insight Cache" on page 679.

Uninstalling a Symantec Endpoint Protection Security Virtual Appliance

You should use the command-line installation tool that Symantec supplies to uninstall a Security Virtual Appliance.

Note: Do not manually remove a Symantec Endpoint Protection Security Virtual Appliance. Use the Symantec Security Virtual Appliance installation tool to uninstall the Security Virtual Appliance. If you manually remove the Security Virtual Appliance, it does not unregister the Security Virtual Appliance from the VMware vShield Manager. This failure to unregister causes issues if you subsequently try to reinstall the Security Virtual Appliance.

To install or to uninstall the Security Virtual Appliance, the vCenter Administrator account that you use must have permissions in the following privilege categories:

- Datastore (All privileges)
- Network (All privileges)
- vApp (All privileges)
- Virtual Machine (All privileges)
- Global > Cancel Task

To uninstall Security Virtual Appliances

1   Navigate to the directory where you invoked the `Symantec_SVA_Install.jar` tool to install the Security Virtual Appliance.

2   Type the following command:

    ```
    java -jar Symantec_SVA_Install.jar -s
    pathname/SVA_InstallSettings.xml -uninstall
    ```

Errors and other command output are written to the `SVA_Install.log` log file. This file is created in the same directory from which you executed the `Symantec_SVA_Install.jar` file command.

Note: In a few instances, the write to that directory may fail. In these cases, then the file is written to the /temp directory and is named SVA_Installxxx.log, where the system replaces xxx with a random number.

See "About vShield-enabled Shared Insight Cache event logging" on page 682.

Using Virtual Image Exception

This chapter includes the following topics:

- Using the Virtual Image Exception tool on a base image

- System requirements for the Virtual Image Exception tool

- Running the Virtual Image Exception tool

- Configuring Symantec Endpoint Protection to bypass the scanning of base image files

Using the Virtual Image Exception tool on a base image

You can use the Virtual Image Exception tool on a base image before you build out your virtual machines. The Virtual Image Exception tool lets your clients bypass the scanning of base image files for threats, which reduces the resource load on disk I/O. It also improves CPU scanning process performance in your virtual desktop infrastructure.

Symantec Endpoint Protection supports the use of the Virtual Image Exception tool for managed clients and unmanaged clients

Note: You cannot use the Virtual Image Exception tool in a non-virtual environment.

Table 30-1   Process for using the Virtual Image Exception tool on a base image

Step	Action
Step 1	On the base image, perform a full scan all of the files to ensure that the files are clean.
	If the Symantec Endpoint Protection client quarantines infected files, you must repair or delete the quarantined files to remove them from quarantine.
	See "Specify when quarantined files are automatically deleted" on page 365.
Step 2	Ensure that the client's quarantine is empty.
	See "Using the Risk log to delete quarantined files on your client computers" on page 367.
Step 3	Run the Virtual Image Exception tool from the command line to mark the base image files.
	See "Running the Virtual Image Exception tool" on page 687.
	See vietool on page 1118.
Step 4	Enable the feature in Symantec Endpoint Protection Manager so that your clients know to look for and bypass the marked files when a scan runs.
	See "Configuring Symantec Endpoint Protection to bypass the scanning of base image files" on page 687.
Step 5	Remove the Virtual Image Exception tool from the base image.

The Virtual Image Exception tool supports fixed, local drives. It works with the files that conform to the New Technology File System (NTFS) standard.

See "System requirements for the Virtual Image Exception tool" on page 686.

System requirements for the Virtual Image Exception tool

The Virtual Image Exception tool is supported for use on VMware ESX, Microsoft Hyper-V, and Citrix Zen desktop platforms.

The client must meet all of the following requirements:

- The client must be installed in one of the supported virtual environments.

- The client must run Symantec Endpoint Protection client software version 12.1 or later.

For the most up-to-date information about requirements and supported platforms, see the following Web page:

Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

See "Using the Virtual Image Exception tool on a base image" on page 685.

Running the Virtual Image Exception tool

Before you run the Virtual Image Exception tool, ensure that you have met all of the system requirements.

See "System requirements for the Virtual Image Exception tool" on page 686.

To run the Virtual Image Exception tool

1   From the Symantec Endpoint Protection Tools product disc, download the following file to the base image:

    `/Virtualization/VirtualImageException/vietool.exe`

2   Open a command prompt with administrative privileges.

3   Run the Virtual Image Exception tool with the proper arguments.

    For example, type: `vietool c: --generate`

See vietool on page 1118.

Configuring Symantec Endpoint Protection to bypass the scanning of base image files

After you run the Virtual Image Exception tool on base image files, you can enable the use of Virtual Image Exceptions in Symantec Endpoint Protection Manager. Once the feature is enabled, virtual clients look for the attribute that the tool inserted. Symantec Endpoint Protection then skips the scanning of base image files that contain the attribute.

You can bypass the scanning of unchanged base image files for Auto-Protect scanning or administrator-defined scans (such as manual scans or scheduled scans).

To configure Symantec Endpoint Protection to use Virtual Image Exception to bypass the scanning of base image files

1   On the console, open the appropriate Virus and Spyware Protection policy.

2   Under **Advanced Options**, click **Miscellaneous**.

3   On the **Virtual Images** tab, check the options that you want to enable.

4   Click **OK**.

See "Using the Virtual Image Exception tool on a base image" on page 685.

Chapter 31

Non-persistent virtual desktop infrastructures

This chapter includes the following topics:

- Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures

- Setting up the base image for non-persistent guest virtual machines in virtual desktop infrastructures

- Creating a registry key to mark the base image Guest Virtual Machines (GVMs) as non-persistent clients

- Configuring a separate purge interval for offline non-persistent VDI clients

Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures

You can configure the Symantec Endpoint Protection client in your base image to indicate that it is a non-persistent virtual client. You can then configure a separate purge interval in Symantec Endpoint Protection for the offline guest virtual machines (GVMs) in non-persistent virtual desktop infrastructures. Symantec Endpoint Protection Manager removes the non-persistent GVM clients that have been offline longer than the specified time period. This feature makes it simpler to manage the GVMs in Symantec Endpoint Protection Manager.

Table 31-1   Tasks to use Symantec Endpoint Protection in non-persistent virtual desktop infrastructures

Step	Description
Step 1	Set up the base image. See "Setting up the base image for non-persistent guest virtual machines in virtual desktop infrastructures" on page 690.
Step 2	In Symantec Endpoint Protection Manager, configure a separate purge interval for offline non-persistent VDI clients. See "Configuring a separate purge interval for offline non-persistent VDI clients" on page 691.

Setting up the base image for non-persistent guest virtual machines in virtual desktop infrastructures

You can set your base image up to make it simpler to use Symantec Endpoint Protection Manager to manage GVMS in non-persistent virtual desktop infrastructures.

Table 31-2   Setting up the base image for non-persistent guest virtual machines in virtual desktop infrastructures

Step	Description
Step 1	Install Symantec Endpoint Protection on the base image. See "About client deployment methods" on page 131.
Step 2	In Symantec Endpoint Protection Manager, disable Tamper Protection so that you can modify the registry. See "Changing Tamper Protection settings" on page 412.
Step 3	Create a registry key on the base image to mark the GVMs as non-persistent clients. See " Creating a registry key to mark the base image Guest Virtual Machines (GVMs) as non-persistent clients" on page 691.
Step 4	In Symantec Endpoint Protection Manager, enable Tamper Protection again. See "Changing Tamper Protection settings" on page 412.

After you have finished setting up the base image, you can configure a separate purge interval for non-persistent clients in Symantec Endpoint Protection Manager.

See "Configuring a separate purge interval for offline non-persistent VDI clients" on page 691.

See "Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures" on page 689.

Creating a registry key to mark the base image Guest Virtual Machines (GVMs) as non-persistent clients

You must create a registry key in the base image to mark the guest virtual machines (GVMs) as non-persistent clients.

To create a registry key to mark the base image GVMs as non-persistent clients

1   After you have installed the Symantec Endpoint Protection client and disabled Tamper Protection, open the registry editor on the base image.

2   Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\.

3   Create a new key named Virtualization.

4   Under Virtualization, create a key of type DWORD named **IsNPVDIClient** and set it to a value of 1.

See "Setting up the base image for non-persistent guest virtual machines in virtual desktop infrastructures" on page 690.

Configuring a separate purge interval for offline non-persistent VDI clients

Over time, obsolete clients can accumulate in the Symantec Endpoint Protection Manager database. Obsolete clients are those clients that have not connected to Symantec Endpoint Protection Manager for 30 days. Symantec Endpoint Protection Manager purges obsolete clients every 30 days by default.

If you do not want to wait the same number of days to purge obsolete non-persistent clients, you can configure a separate interval for them. If you do not configure a separate interval, then offline non-persistent VDI clients are purged at the same interval that non-virtual obsolete clients are purged.

Note: Online non-persistent clients count toward the number of deployed licenses; offline non-persistent clients do not.

You can also filter the offline non-persistent clients out of the view on the **Clients** page.

To configure the purge interval for offline non-persistent VDI clients

1   In the Symantec Endpoint Protection Manager console, on the **Admin** page, click **Domains**.

2   In the **Domains** tree, click the desired domain.

3   Under **Tasks**, click **Edit Domain Properties**.

4   On the **Edit Domain Properties > General** tab, check the **Delete non-persistent VDI clients that have not connected for specified time** checkbox and change the **days** value to the desired number.

    The **Delete clients that have not connected for specified time** option must be checked to access the option for offline non-persistent VDI clients.

5   Click **OK**.

See "Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures" on page 689.

Section 5

Configuring and managing Symantec Endpoint Protection Manager

Managing the connection between the management server and the client computers

This chapter includes the following topics:

Managing the client-server connection

After you install the client, the management server automatically connects to the client computer. You may need to verify whether the client and server communicate.

You may also want to configure the connection between the server and client.

Table 32-1 lists the tasks you can perform to view and manage how the management server connects to clients.

Table 32-1   Tasks to manage connections between the management server and the clients

Action	Description
Check whether the client is connected to the management server	You can check the client status icon in the client and in the management console. The status icon shows whether the client and the server communicate.
	See "How to determine whether the client is connected in the console" on page 224.
	A computer may have the client software installed, but does not have the correct communications file.
	See "Why do I need to replace the client-server communications file on the client computer?" on page 698.
	See "How do I replace the client-server communications file on the client computer?" on page 700.
Check that the client gets policy updates	Check that the client computers get the most current policy updates by checking the policy serial number in the client and in the management console. The policy serial number should match if the client can communicate with the server and receives regular policy updates.
	You can perform a manual policy update and then check the policy serial numbers against each other.
	See "Using the policy serial number to check client-server communication" on page 309.
	See "Manually updating policies on the client" on page 310.
Change which method you use to download policies and content to the clients	You can configure the management server to push down policies to the client or for the clients to pull the policies from the management server.
	See "Configuring push mode or pull mode to update client policies and content" on page 308.

Table 32-1 Tasks to manage connections between the management server and the clients *(continued)*

Action	Description
Decide whether to use the default management server list	You can work with an alternative list of management servers for failover and load balancing. The management server list provides a list of multiple management servers that clients can connect to. See "Configuring a management server list" on page 740.
Configure communication settings for a location	You can configure separate communication settings for locations and for groups. See "Configuring communication settings for a location" on page 259.
Troubleshoot management server connectivity problems	If the management server and the client do not connect, you can troubleshoot connection problems. See "Troubleshooting communication problems between the management server and the client" on page 756.

If you have Symantec Network Access Control installed, you can also configure the connection between the management server and Enforcers.

For more information on the ports that Symantec Endpoint Protection uses, see the knowledge base article: Which Communications Ports does Symantec Endpoint Protection use?

How to determine whether the client is connected and protected

You can check the notification area icon on the client to determine whether the client is connected to a management server and adequately protected.

The icon is located in the lower-right hand corner of the client computer desktop. You can also right-click this icon to display frequently used commands.

Table 32-2 Symantec Endpoint Protection client status icons

Icon	Description
🛡️	The client runs with no problems. It is either offline or unmanaged. Unmanaged clients are not connected to a management server. The icon is a plain yellow shield.
🛡️	The client runs with no problems. It is connected to and communicates with the server. All components of the security policy protect the computer. The icon is a yellow shield with a green dot.

Table 32-2 Symantec Endpoint Protection client status icons *(continued)*

Icon	Description
	The client has a minor problem. For example, the virus definitions may be out of date. The icon is a yellow shield and a light yellow dot that contains a black exclamation mark.
	The client does not run, has a major problem, or has at least one protection technology disabled. For example, Network Threat Protection may be disabled. The icon is a yellow shield with a white dot outlined in red and a red line across the dot.

Table 32-3 displays the Symantec Network Access Control client status icons that appear in notification area.

Table 32-3 Symantec Network Access Control client status icons

Icon	Description
	The client runs with no problems and has both passed the Host Integrity check and updated the security policy. It is either offline or unmanaged. Unmanaged clients are not connected to a management server. The icon is a plain gold key.
	The client runs with no problems and has both passed the Host Integrity check and updated the security policy. It communicates with the server. The icon is a gold key with a green dot.
	The client has either failed the Host Integrity check or has not updated the security policy. The icon is a gold key with a red dot that contains a white "x."

You can also check the management server to view the connection status of the computers.

See "How to determine whether the client is connected in the console" on page 224.

See "Viewing the status of deployed client computers" on page 611.

See "Managing the client-server connection" on page 696.

Why do I need to replace the client-server communications file on the client computer?

Symantec Endpoint Protection Manager connects to the client with a communications file called Sylink.xml. The Sylink.xml file includes the communication settings such as the IP address of the management server and

the heartbeat interval. After you install a client installation package on to the client computers, the client and the server automatically communicate.

Normally you do not need to replace the Sylink.xml file. However, you may need to replace the existing Sylink.xml file on the client computer in the following situations:

■ The client and the server do not communicate. If the clients have lost the communication with the management server, you must replace the old Sylink.xml file with a new file.
  See "Managing the client-server connection" on page 696.
  See "Checking the connection to the management server on the client computer" on page 759.

■ You want to convert an unmanaged client to a managed client. If a user installs a client from the product disc, the client is unmanaged and does not communicate with the management server. You can also reinstall the client software on the computer as a managed computer.
  See "About managed and unmanaged clients" on page 146.

■ You want to manage a previously orphaned client. For example, if the hard drive that the management server is installed on gets corrupted, you must reinstall the management server. You can update the Sylink.xml file to re-establish communication with all your orphaned clients.
  See "Disabling or enabling secure communications between the server and the client" on page 712.

■ You want to move a large number of clients from multiple groups to a single group. For example, you might want to move the client computers in a remote group and a laptop group to a test group. Typically, you need to move the client computers one group at a time.
  See "Moving a client computer to another group" on page 219.

■ To install a Security Virtual Appliance in a VMware vShield environment. To install a Security Virtual Appliance, you must export the communications file manually.
  See "What do I need to do to install a Security Virtual Appliance?" on page 669.
  See "Exporting the client-server communications file manually" on page 702.

See "How do I replace the client-server communications file on the client computer?" on page 700.

See "Restoring client-server communications by using a client installation package" on page 701.

How do I replace the client-server communications file on the client computer?

If you need to replace the client-server communications file (Sylink.xml) on the client computer, you can use the following methods:

- Create a new client installation package and deploy it on the client computers. Use this method if manually importing the Sylink.xml on large environment is physically not possible and requires administrative access.
  See "Restoring client-server communications by using a client installation package" on page 701.

- Write a script that runs the SylinkDrop tool, which is located in the /Tools folder of the Tools product disc. Symantec recommends this method for a large number of clients. You should also use the SylinkDrop tool if you use a software management tool to download the client software to computers. The advantage of the software management tool is that it downloads the Sylink.xml file as soon as the end user turns on the client computer. In comparison, the client installation package downloads the new Sylink.xml file only after the client computer connects to the management server.
  See "Restoring client-server communication settings by using the SylinkDrop tool" on page 764.

- Export the Sylink.xml file to the client computer and import it on the client computer manually. Symantec recommends this method if you want to use a software management tool like Altiris. With a software management tool, the job is queued up and completed whenever the users turn on their computer. With the other methods, the client computer must be online.
  Table 32-4 displays the process for exporting and importing the Sylink.xml file into the client computer.

Table 32-4   Steps for exporting and importing the communications file

Step	Task	Description
Step 1	Export a file that includes all the communication settings for the group that you want the client to be in.	The default file name is *group name*_sylink.xml. See "Exporting the client-server communications file manually" on page 702.
Step 2	Deploy the file to the client computer.	You can either save the file to a network location or send it to an individual user on the client computer.

Table 32-4   Steps for exporting and importing the communications file
                    (continued)

Step	Task	Description
Step 3	Import the file on the client computer.	Either you or the user can import the file on the client computer. See "Importing client-server communication settings into the client" on page 704. Unmanaged clients are not password-protected, so you do not need a password on the client. However, if you try to import a file into a managed client that is password-protected, then you must enter a password. The password is the same one that is used to import or export a policy. See "Password-protecting the client" on page 245. You do not need to restart the client computer.
Step 4	Verify client and server communication on the client.	The client immediately connects to the management server. The management server places the client in the group that is specified in the communication file. The client is updated with the group's policies and settings. After the client and the management server communicate, the notification area icon with the green dot appears in the client computer's taskbar. See "How to determine whether the client is connected in the console" on page 224.

See "Client and server communication files" on page 769.

See "Why do I need to replace the client-server communications file on the client computer?" on page 698.

Restoring client-server communications by using a client installation package

If the client-server communications breaks, you can quickly restore communications by replacing the Sylink.xml file on the client computer. You can replace the sylink.xml file by redeploying a client installation package. Use this method for a large number of computers, for the computers that you cannot physically access easily, or the computers that require administrative access.

See "Why do I need to replace the client-server communications file on the client computer?" on page 698.

To restore client-server communication settings by using a client installation package

1   On the **Home** page, in the **Common Tasks** drop-down list, click **Install protection client to computers**.

2   In the **Client Deployment Wizard**, click **Communication Update Package Deployment**, and then click **Next**.

3   Select from the following options, and then click **Next**.

■   The group of computers on which you want to deploy the client installation package.

■   The policy mode that applies to the protected computer.

■   The password to stop the client service, or import or export a policy, if you previously set one.
See "Password-protecting the client" on page 245.

4   Choose one of the following deployment methods, and then click **Next**:

■   Click **Remote Push** and go to step 5 in the following procedure.
See "Deploying clients by using Remote Push" on page 135.

■   **Save Package** and go to step 5 in the following procedure.
See "Deploying clients by using Save Package" on page 137.

5   Confirm that the computer users installed the custom installation package.

You or the computer users must restart the client computers.

See "Viewing the status of deployed client computers" on page 611.

See "Restarting client computers" on page 145.

Exporting the client-server communications file manually

If the client and server do not communicate, you may need to reinstall the Sylink.xml file on the client computer to restore communications. You can manually export the Sylink.xml file from Symantec Endpoint Protection Manager on a group basis.

The most common reasons for replacing the Sylink.xml are:

■   To convert an unmanaged client into a managed client.

■   To reconnect a previously orphaned client to the management server.

See "Disabling or enabling secure communications between the server and the client" on page 712.

■ To install a Security Virtual Appliance in a VMware vShield environment.
See "What do I need to do to install a Security Virtual Appliance?" on page 669.

See "Why do I need to replace the client-server communications file on the client computer?" on page 698.

If you need to update client-server communications for a large number of clients, redeploy the client installation package instead of using this method.

See "Restoring client-server communications by using a client installation package" on page 701.

To export the client-server communications file manually

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

2   Under **View Clients**, select the group in which you want the client to appear.

3   Right-click the group, and then click **Export Communication Settings**.

4   In the Export Communication Settings for *group name* dialog box, click **Browse**.

5   In the **Select Export File** dialog box, locate the folder to where you want to export the .xml file, and then click **OK**.

6   In the **Export Communication Settings for *group name*** dialog box, select one of the following options:

   ■ To apply the policies from the group from which the computer is a member, click **Computer Mode**.

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

7   Click **Export**.

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

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

See "Importing client-server communication settings into the client" on page 704.

Importing client-server communication settings into the client

Once you have exported client-server communication settings, you can import them into a client. You can use it to convert an unmanaged client into a managed client or to reconnect a previously orphaned client with a Symantec Endpoint Protection Manager.

To import the client-server communications settings file into the client

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

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

3   In the **Troubleshooting** dialog box, in the **Management** pane, click **Import**.

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

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

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

See "Exporting the client-server communications file manually" on page 702.

Configuring SSL between Symantec Endpoint Protection Manager and the clients

Symantec Endpoint Protection Manager uses an Apache Web site to communicate with clients and provide reporting services. The Web site uses HTTP for all communications. HTTP is an unencrypted protocol and does not provide for the confidentiality or integrity of the communications over it. You can configure the Symantec Endpoint Protection Manager Apache Web site to use a Secure Sockets Layer (SSL) certificate to sign and encrypt data using an HTTPS connection.

Table 32-5   Configuring SSL communication to the client

Step	Action	Description
1	Check that the default SSL port is available	In some networks, port 433 may already be bound to another application or service. Before you enable SSL communication, you must check to see if the default port (433) is available. See "Verifying port availability" on page 705.
2	Change the default SSL port as needed	If port 433 is not available, choose an unused port from the high port range (49152-65535). Adjust the server configuration to use the new port. See "Changing the SSL port assignment" on page 706.
3	Enable SSL communication to the client	Edit the Apache httpd.config file to allow SSL communication to the client. By default, SSL traffic uses port 433. You may need to change the default port if it is already used. See "Enabling SSL communication between the management server and the client" on page 706.

See "Supported and unsupported migration paths to Symantec Endpoint Protection" on page 179.

See "Migrating from Symantec AntiVirus or Symantec Client Security" on page 177.

Verifying port availability

Some Symantec Endpoint Protection Manager configurations require that you change a default port assignment to prevent a conflict with other applications or services. Before you assign a new port, you must check to be sure that the new port is not already used.

To verify port availability

1 Open a command prompt and execute the command:

```
netstat -an
```

2 In the Local Address column, look for an entry that ends with the port number you want to check.

For instance, to see if port 443 is available, look in the Local Address column for an entry that ends in 443. If no entry ends in 443, the port is available.

See "Configuring SSL between Symantec Endpoint Protection Manager and the clients" on page 704.

Changing the SSL port assignment

You may be required to change the default SSL port assignment if the default SSL port is not available.

You must first verify that the new SSL port that you choose is unused.

See "Verifying port availability" on page 705.

To change the SSL port assignment

1   In a text editor, open the following file:

    %SEPM%\apache\conf\ssl\sslForClients.conf

2   Edit the string, Listen 443 with the new port number. For instance, if the new port number is 53300, the edited string becomes Listen 53300.

3   Save the file and close the text editor.

4   Restart the Symantec Endpoint Protection Manager.

5   To verify that the new port works correctly, in a Web browser, enter the following URL:

    https://ServerHostName:<new port
    number>/secars/secars.dll?hello.secars.

    In the URL, ServerHostName is the computer name for the Symantec Endpoint Protection Manager. If the word "hello" is displayed, the port change is successful. If a page error is displayed, repeat the first steps and verify that the string is formatted correctly. Also check that you enter the URL correctly.

6   In the console, on the **Policies** tab, click **Policy Components > Management Server Lists**.

7   In the management server list, click on the management server being configured to use SSL and then click **Edit**.

8   In the **Edit Management Server** window, click **Customize HTTPS port** and then enter the new port number.

9   Click **OK**.

    See "Enabling SSL communication between the management server and the client" on page 706.

Enabling SSL communication between the management server and the client

You edit the httpd.config file to enable Secure Sockets Layer (SSL) communication between the Symantec Endpoint Protection Manager and the clients.

Enabling SSL communication between the management server and the client

1 In a text editor, open the file %SEPM%\apache\conf\httpd.conf.

2 Find the following entry:

    #Include conf/ssl/sslForClients.conf

3 Remove the hash mark (#) from the text string and then save the file.

4 Restart the Symantec Endpoint Protection Manager.

See "Stopping and starting the management server service" on page 170.

See "Stopping and starting the Apache Web server" on page 761.

See "Configuring SSL between Symantec Endpoint Protection Manager and the clients" on page 704.

Improving client and server performance

Symantec Endpoint Protection Manager includes various features that enable you to increase the client performance and server performance while still maintaining a high level of security.

Table 32-6   Tasks to improve performance on the server and on the client

Task	Description
Change client-server communication settings	Use pull mode instead of push mode to control how often the management server downloads policies and content updates to the client computers. In pull mode, the management server can support more clients.
	Increase the heartbeat interval so that the client and the server communicate less frequently. For fewer than 100 clients per server, increase the heartbeat to 15-30 minutes. For 100 to 1,000 clients, increase the heartbeat to 30-60 minutes. Larger networks might need a longer heartbeat interval. Increase the download randomization to between one and three times the heartbeat interval.
	See "Configuring push mode or pull mode to update client policies and content" on page 308.
	For more information about setting heartbeat intervals, see the Symantec Endpoint Sizing and Scalability Best Practices white paper.

Table 32-6   Tasks to improve performance on the server and on the client
(continued)

Task	Description
Randomize and reduce the number of content updates	Content updates vary in size and frequency, depending on the content type and availability. You can reduce the effect of downloading and importing a full set of content updates by using the following methods: ■ Distribute the client load across multiple management servers. See "Configuring a management server list" on page 740. ■ Use alternative methods to distribute the content, such as a Group Update Provider or third-party distribution tools. A Group Update Provider helps you conserve bandwidth by offloading processing power from the server to a client that downloads the content. See "Using Group Update Providers to distribute content to clients " on page 580. See "Using third-party distribution tools to update client computers" on page 594. ■ Randomize the time when LiveUpdate downloads content to the client computers. See "Randomizing content downloads from a LiveUpdate server" on page 573. See "Randomizing content downloads from the default management server or a Group Update Provider" on page 573. ■ Download content updates when users are not actively using the client computer. See "Configuring client updates to run when client computers are idle" on page 574.
Adjust scans to improve computer performance	You can change some scan settings to improve the computers' performance without reducing protection. For example, you can configure scans to ignore trusted files or to run when the computer is idle. See "Adjusting scans to improve computer performance" on page 346. See "Customizing Auto-Protect for Windows clients" on page 378.

Task	Description
Reduce database client log volume	You can configure the logging options to optimize storage requirements and comply with company policies that control retention of logged data.
	The database receives and stores a constant flow of entries into its log files. You must manage the data that is stored in the database so that the stored data does not consume all the available disk space. Too much data can cause the computer on which the database runs to crash.
	You can reduce the volume of log data by performing the following tasks:
	■ Upload only some of the client logs to the server, and change the frequency with which the client logs are uploaded. See "Specifying client log size and which logs to upload to the management server" on page 731.
	■ Specify how many log entries the client computer can keep in the database, and how long to keep them. See "Specifying how long to keep log entries in the database" on page 732.
	■ Filter the less important risk events and system events out so that less data is forwarded to the server. See "Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers" on page 386.
	■ Reduce the number of clients that each management server manages. See "Configuring a management server list" on page 740. See "Installing Symantec Endpoint Protection Manager" on page 95.
	■ Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server. See "Configuring push mode or pull mode to update client policies and content" on page 308.
	■ Increase the amount of hard disk space in the directory where the log data is stored before being written to the database. See "About increasing the disk space on the server for client log data" on page 733.
Perform database maintenance tasks	To increase the speed of communication between the client and the server, you should schedule regular database maintenance tasks.
	See "Scheduling automatic database maintenance tasks" on page 726.

About server certificates

Certificates are the industry standard for authenticating and encrypting sensitive data. To prevent the reading of information as it passes through routers in the network, data should be encrypted.

To communicate with the clients, the management server uses a server certificate. For the management server to identify and authenticate itself with a server certificate, Symantec Endpoint Protection Manager encrypts the data by default. However, there are situations where you must disable encryption between the server and the client.

See "Best practices for updating server certificates and maintaining the client-server connection" on page 710.

See "Disabling or enabling secure communications between the server and the client" on page 712.

You may also want to back up the certificate as a safety precaution. If the management server is damaged or you forget the keystore password, you can easily retrieve the password.

See "Backing up a server certificate" on page 746.

See "Updating or restoring a server certificate" on page 713.

The management server supports the following types of certificates:

- JKS Keystore file (.jks) (default)
  A Java tool that is called keytool.exe generates the keystore file. The Java Cryptography Extension (.jceks) format requires a specific version of the Java Runtime Environment (JRE). The management server supports only a .jceks keystore file that is generated with the same version as the Java Development Kit on the management server.
  The keystore file must contain both a certificate and a private key. The keystore password must be the same as the key password. You can locate the password in the following file:
  `Drive:\\Program Files\Symantec\ Symantec Endpoint Protection Manager\Server Private Key Backup\recovery_timestamp.zip`. The password appears in the `keystore.password=` line.

- PKCS12 keystore file (.pfx and .p12)

- Certificate and private key file (.der and .pem format)
  Symantec supports unencrypted certificates and private keys in the .der or the .pem format. .Pkcs8-encrypted private keys are not supported.

Best practices for updating server certificates and maintaining the client-server connection

You may need to update the security certificate in the following situations:

- You restore a previous security certificate that the clients already use.

■ You want to use a different security certificate than the default certificate (.jks).

When clients use secure communication with the server, the server certificate is exchanged between the server and the clients. This exchange establishes a trust relationship between the server and clients. When the certificate changes on the server, the trust relationship is broken and clients no longer can communicate. This problem is called orphaning clients.

Note: Use this process to update either one management server or multiple management servers at the same time.

Table 32-7 lists the steps to update the certificate without orphaning the clients that the server manages.

Table 32-7   Steps to update server certificates

Step	Task	Description
1	Disable server certificate verification	Disable secure communications between the server and the clients. When you disable the verification, the clients stay connected while the server updates the server certificate.
		See "Disabling or enabling secure communications between the server and the client" on page 712.
2	Wait for all clients to receive the updated policy	The process of deploying the updated policy may take a week or longer, depending on the following factors:
		■ The number of clients that connect to the management server. Large installations may take several days to complete the process because the managed computers must be online to receive the new policy.
		■ Some users may be on vacation with their computers offline.
		See "Using the policy serial number to check client-server communication" on page 309.
3	Update the server certificate	Update the server certificate. If you migrate or upgrade the management server, upgrade the certificate first.
		See "Upgrading a management server" on page 166.
		See "Updating or restoring a server certificate" on page 713.
4	Enable server certificate verification again	Enable secure communications between the server and the clients again.
		See "Disabling or enabling secure communications between the server and the client" on page 712.

Step	Task	Description
		Table 32-7 Steps to update server certificates *(continued)*
5	Wait for all clients to receive the updated policy	The client computers must receive the policy changes from the previous step.
6	Restore replication relationship (optional)	If the server you updated replicates with other management servers, restore the replication relationship. See "Turning on replication after upgrade" on page 169.

Disabling or enabling secure communications between the server and the client

To authenticate communication between the management server and the client, the server uses a certificate. If the certificate is corrupted or invalid, the clients cannot communicate with the server. If you disable secure communications, then the clients can still communicate with the server. However, the clients do not authenticate communications from the management server.

You should temporarily disable secure communications between the clients and server for the following reasons:

- To move a large number of clients from one site to another site without needing to use the Sylink.xml file.
  See "Why do I need to replace the client-server communications file on the client computer?" on page 698.

- To update a corrupted certificate or invalid certificate. You can update multiple management servers at the same time. As a best practice, you should perform disaster recovery instead.
  See "Updating or restoring a server certificate" on page 713.
  See "Performing disaster recovery" on page 749.

Make sure that you configure this setting for the groups that do not inherit from a parent group.

After you move the clients or update the certificate, you enable secure communications again.

Disabling or enabling secure communications between the server and the client

1   On the console, click **Clients** > **Policies** > **General Settings**.

2   On the **Security Settings** tab, check or uncheck **Enable secure communications between the management server and clients by using digital certificates for authentication**.

3   Click **OK**.

See "About server certificates" on page 709.

See "Best practices for updating server certificates and maintaining the client-server connection" on page 710.

Updating or restoring a server certificate

The server certificate encrypts and decrypts files between the server and the client. The client connects to the server with an encryption key, downloads a file, and then decrypts the key to verify its authenticity. If you change the certificate on the server without manually updating the client, the encrypted connection between the server and the client breaks.

You must update the server certificate in the following situations:

■   You reinstall Symantec Endpoint Protection Manager without using the recovery file. You update the certificate to restore a previous certificate that clients already use.
    See "Installing Symantec Endpoint Protection Manager" on page 95.

■   You replace one management server with another management server and use the same IP and server name.

■   You apply the wrong server certificate (.JKS) after disaster recovery.

■   You purchased a different certificate and want to use that certificate instead of the default .JKS certificate.
    See "About server certificates" on page 709.

■   You upgraded from a legacy 11.x management server.
    See "Upgrading a management server" on page 166.

See "Best practices for updating server certificates and maintaining the client-server connection" on page 710.

To update or restore a server certificate

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

2   Under **Servers**, under **Local Site**, click the management server for which you want to update the server certificate.

3 Under **Tasks**, click **Manage Server Certificate**, and then click **Next**.

4 In the **Manage Server Certificate** panel, click **Update the server certificate**, click **Next**, and then click **Yes**.

To maintain the server-client connection, disable secure connections.

See "Disabling or enabling secure communications between the server and the client" on page 712.

5 In the **Update Server Certificate** panel, choose the certificate you want to update to, and then click **Next**:

6 For each certificate type, following the instructions on the panels, and click **Finish**.

Backup server certificates are in `Drive:\\Program Files\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup\recovery_timestamp.zip`. You can locate the password for the keystore file in the `settings.properties` file within the same `.zip` file. The password appears in the `keystore.password=` line.

7 You must log off and restart the management server for the certificate to become effective.

See "Stopping and starting the management server service" on page 170.

Configuring the management server

This chapter includes the following topics:

- Managing Symantec Endpoint Protection Manager servers and third-party servers

- About the types of Symantec Endpoint Protection servers

- Exporting and importing server settings

- Enabling or disabling Symantec Endpoint Protection Manager web services

Managing Symantec Endpoint Protection Manager servers and third-party servers

You can configure Symantec Endpoint Protection Manager to integrate with many of the different types of servers in your network environment.

Table 33-1   Server management

Task	Description
Learn about servers	Decide which types of servers you need to set up.
	See "About the types of Symantec Endpoint Protection servers" on page 718.

Table 33-1   Server management *(continued)*

Task	Description
Set server communication permissions	You can allow or deny access to the remote console. You manage access by adding exceptions based on the IP address of a single computer or a group of computers. See "Granting or blocking access to remote Symantec Endpoint Protection Manager consoles" on page 102.
Modify server settings	To modify database settings, or to restore your database on a different computer, you can modify server settings. See "Reinstalling or reconfiguring Symantec Endpoint Protection Manager" on page 750.
Configure the mail server	To work with a specific mail server in your network, you need to configure the mail server. See "Establishing communication between the management server and email servers" on page 640.
Manage directory servers	You can integrate Symantec Endpoint Protection with directory servers to help manage administrator accounts or to create organizational units. See "Connecting Symantec Endpoint Protection Manager to a directory server" on page 213.
Configure proxy settings if you use a proxy server to connect to Symantec LiveUpdate servers	To set up the Symantec Endpoint Protection Manager to connect to the Internet through a proxy server, you must configure the proxy server connection. See "Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate" on page 564.
Import or export server properties	You can export server settings to an xml file, and you can re-import the same settings. See "Exporting and importing server settings" on page 719.

Table 33-1 Server management *(continued)*

Task	Description
Manage server certificates	The Symantec Endpoint Protection Manager server uses a server certificate to encrypt data for the communication between all servers, clients, and optional Enforcers in a network. The server identifies and authenticates itself with a server certificate. You may need to back up, update, or generate a new server certificate. See "About server certificates" on page 709. See "Updating or restoring a server certificate" on page 713. See "Backing up a server certificate" on page 746. See "Generating a new server certificate" on page 751.
Configure SecurID Authentication for a server	If you choose to authenticate administrator accounts by using RSA SecurID, you must also configure the management server to communicate with the RSA server. See "Configuring the management server to authenticate administrators who use RSA SecurID to log on" on page 277.
Move the server to a different computer	You may need to move the management server software from one computer to another for the following reasons: ■ You must move the management server from a test environment to a production environment. ■ The computer on which the management server runs has a hardware failure. You can move the management server software in the following ways: ■ Install the management server on another computer and perform replication. See "Re-adding a replication partner that you previously deleted" on page 197. ■ Install the management server on another computer using the recovery file. See "Reinstalling or reconfiguring Symantec Endpoint Protection Manager" on page 750.
Start and stop the management server	The management server runs as an automatic service. You must stop the management server service when you upgrade, or perform disaster recovery. See "Stopping and starting the management server service" on page 170.

About the types of Symantec Endpoint Protection servers

The following definitions may be helpful to understand when managing servers:

- Site
  A site consists of one or more management servers and one database (the embedded database or Microsoft SQL Server) typically located together at the same business location. The site to which you log on is the local site, and you can modify it directly. Any site other than the local site is referred to as a remote site. You connect sites by using replication.
  See "Setting up sites and replication" on page 187.

- Management server
  The computer on which the Symantec Endpoint Protection Manager software is installed. From the management server, policies can be created and assigned to different organizational groups. You can monitor clients, view reports, logs, and alerts, and configure servers and administrator accounts. Multiple management servers at a single site provide failover and load balancing capabilities.
  See "Setting up failover and load balancing" on page 737.

- Database server
  The database used by Symantec Endpoint Protection Manager. There is one database per site. The database can be on the same computer as the management server or on a different computer if you use a SQL Server database.
  See "Maintaining the database" on page 721.

- Symantec Network Access Control Enforcer
  An Enforcer is used by Symantec Network Access Control to allow or deny access to the enterprise network. Symantec Network Access Control includes the following types of Enforcers: Gateway Enforcer, LAN Enforcer, and Integrated Enforcer.
  See "About Symantec Network Access Control" on page 780.

- Replication partner
  A relationship created between two sites to enable data replication between them.

Exporting and importing server settings

The server properties file includes the server settings for Symantec Endpoint Protection Manager. You may need to export and import the server properties file in the following situations:

■ You use the disaster recovery file to reinstall Symantec Endpoint Protection Manager.
The disaster recovery file does not include the server settings. When you reinstall Symantec Endpoint Protection Manager, you lose any default server settings that you had previously changed. You can use the exported server properties file to reimport the changed server settings.

■ You install Symantec Endpoint Protection Manager in a test environment and later install the management server in a production environment. You can import the exported server properties file to the production environment.

■ You upgrade the management server from a previous version to a newer version, and you need to import all the policies and locations.

■ You want to export all policies rather than individual policies from one management server to another management server.
See "Exporting and importing individual policies" on page 303.

The server properties file includes all policies, locations, and server settings and uses an .xml format.

See "Managing Symantec Endpoint Protection Manager servers and third-party servers" on page 715.

To export server settings

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

2   Under **Servers**, expand **Local Site (Site *site name*)**, and then select the management server you want to export.

3   Click **Export Server Properties**.

4   Select a location in which to save the file and specify a file name.

5   Click **Export**.

To import server settings

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

2   Under **Servers,** expand **Local Site (Site *site name*)**, and then select the management server for which you want to import settings.

3   Click **Import Server Properties**.

4 Select the file you want to import, and then click **Import**.

5 Click **Yes**.

Enabling or disabling Symantec Endpoint Protection Manager web services

Symantec Endpoint Protection provides two sets of web services on the management server. One set was written to provide integration with Symantec Protection Center. The other set was written to provide support for development of remote management applications.

Both sets of web services are enabled by default. You can enable or disable either set of web services by running a script that is included with the product.

To enable or disable Symantec Endpoint Protection Manager web services

1 In a command window, run the following batch file:

Symantec_Endpoint_Protection_Manager_installation_folder/ToolsConfigSEPM.bat

2 Set any of the following options:

-RmmWS:ON	Enables web services for remote management.
-RmmWS:OFF	Disables web services for remote management.
-SpcWS:ON	Enables web services for internal Symantec tools (Symantec Protection Center).
-SpcWS:OFF	Disables web services for internal Symantec tools (Symantec Protection Center).

Managing databases

This chapter includes the following topics:

- Maintaining the database

- Scheduling automatic database backups

- Scheduling automatic database maintenance tasks

- Exporting data to a Syslog server

- Exporting log data to a text file

- Exporting log data to a comma-delimited text file

- Specifying client log size and which logs to upload to the management server

- Specifying how long to keep log entries in the database

- About increasing the disk space on the server for client log data

- Clearing log data from the database manually

Maintaining the database

Symantec Endpoint Protection supports both an embedded database and the Microsoft SQL Server database. If you have more than 5,000 clients, you should use a Microsoft SQL Server database.

Symantec Endpoint Protection Manager automatically installs an embedded database. The database contains information about security policies, configuration settings, attack data, logs, and reports.

After you install Symantec Endpoint Protection Manager, the management server may start to slow down after a few weeks or a few months. To improve the

management server performance, you may need to reduce the database storage space and schedule various database maintenance tasks.

Table 34-1   Database management tasks

Task	Description
Schedule regular database backups	You should schedule regular database backups in case the database gets corrupted. See "Backing up the database and logs" on page 744. See "Scheduling automatic database backups" on page 725. See "Performing disaster recovery" on page 749. Optionally, to prevent an automatic sweep of the database until after a backup occurs, you can manually sweep data from the database. See "Clearing log data from the database manually" on page 734.
Schedule database maintenance tasks	You can speed up the interaction time between the management server and the database by scheduling database maintenance tasks. You can schedule the management server to perform the following maintenance tasks immediately or when users are not on the client computers. ■ Remove unused data from the transaction log. ■ Rebuild the database table indexes to improve the database's sorting and searching capabilities. See "Scheduling automatic database maintenance tasks" on page 726.
Periodically check the database file size	If you use the Microsoft SQL Server database rather than the embedded database, make sure that the database does not reach the maximum file size. See "Increasing the Microsoft SQL Server database file size" on page 727.

Table 34-1   Database management tasks *(continued)*

Task	Description
Calculate the database storage space that you need	Before you can decide how to reduce the amount of storage space, calculate the total amount of disk space that you need. The database storage is based on the following factors: ■ Log size and expiration time period. ■ The number of client computers. ■ The average number of viruses per month. ■ The number of events you need to retain for each log. ■ The number of content updates. The content updates require about 300 MB each. See "Configuring the disk space that is used for LiveUpdate downloads" on page 571. See "Configuring the content revisions that clients use" on page 570. ■ The number of client versions you need to retain for each language. For example, if you have both 32-bit clients and 64-bit clients, you need twice the number of language versions. ■ The number of backups you need to keep. The backup size is approximately 75 percent of the database size, and then multiplied by the number of backup copies that you keep. For more information on how to calculate the hard disk space you need, see the Symantec white paper, Sizing and Scalability Recommendations for Symantec Endpoint Protection.

Table 34-1 Database management tasks *(continued)*

Task	Description
Reduce the volume of log data	The database receives and stores a constant flow of entries into its log files. You must manage the data that is stored in the database so that the stored data does not consume all the available disk space. Too much data can cause the computer on which the database runs to crash. You can reduce the volume of log data by performing the following tasks: ■ Upload only some of the client logs to the server, and change the frequency with which the client logs are uploaded. See "Specifying client log size and which logs to upload to the management server" on page 731. ■ Specify how many log entries the client computer can keep in the database, and how long to keep them. See "Specifying how long to keep log entries in the database" on page 732. ■ Filter the less important risk events and system events out so that less data is forwarded to the server. See "Modifying miscellaneous settings for Virus and Spyware Protection on Windows computers" on page 386. ■ Reduce the amount of space in the directory where the log data is stored before being inserted into the database. See "About increasing the disk space on the server for client log data" on page 733. ■ Reduce the number of clients that each management server manages. See "Configuring a management server list" on page 740. ■ Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server. See "Configuring push mode or pull mode to update client policies and content" on page 308.
Export log data to another server	For security purposes, you might need to retain the number of log records for a longer period of time. To keep the client log data volume low, you can export the log data to another server. See "Exporting log data to a text file" on page 729. See "Exporting data to a Syslog server" on page 728.
Create client installation packages with only the protection that you need	The more protection features that you install with the client, the more space that the client information takes in the database. Create the client installation package with only the appropriate level of protection the client computer needs. The more groups you add, the more space the client information takes in the database. See "Configuring client installation package features" on page 142.

Task	Description
Use the Group Update Provider to download content	If you have low bandwidth or more than 100 client computers, use Group Update Providers to download content. For example, 2,000 clients using a Group Update Provider is the equivalent of using four to five management servers to download content. See "Using Group Update Providers to distribute content to clients " on page 580. To reduce disk space and database size, you can reduce the number of content revisions that are kept on the server. See "Configuring the disk space that is used for LiveUpdate downloads" on page 571.
Restore the database	You can recover a corrupted database by restoring the database on the same computer on which it was installed originally. Or, you can install the database on a different computer. See "Restoring the database" on page 752.

See "Verifying the connection with the database" on page 767.

The information in the database is stored in tables, also called the database schema. You might need the schema to write queries for customized reports. For more information, see the *Symantec Endpoint Protection Manager Database Schema Reference* at the following location: Symantec Endpoint Protection documentation site.

Scheduling automatic database backups

You can schedule database backups to occur at a time when fewer users are logged on to the network.

You can also back up the database at any time.

See "Backing up the database and logs" on page 744.

To schedule automatic database backups

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

2   Under **Servers**, click the icon that represents the database that you want to back up.

3   Under **Tasks**, click **Edit Database Properties**.

4   In the **Database Properties** dialog box, on the **Backup Settings** tab, do the following tasks.

   ■ In the **Backup server** drop-down list, specify on which management server you want to save the backup.

- Check **Back up logs** if you need to save a copy of the logs for security purposes or company policy.
  Otherwise, leave this option disabled, as logs use a lot of disk space.

- Specify the number of backups if your company policy requires it.

5   Make sure **Schedule Backups** is checked, and set the schedule.

6   Click **OK**.

Scheduling automatic database maintenance tasks

After you install the management server, the space in the database grows continually. The management server slows down after a few weeks or months. To reduce the database size and to improve the response time with the database, the management server performs the following database maintenance tasks:

- Truncates the transaction log.
  The transaction log records almost every change that takes place within the database. The management server removes unused data from the transaction log.

- Rebuilds the index.
  The management server defragments the database table indexes to improve the time it takes to sort and search the database.

By default, the management server performs these tasks on a schedule. You can perform the maintenance tasks immediately, or adjust the schedule so that it occurs when users are not on their computers.

Note: You can also perform the database maintenance tasks in Microsoft SQL Server Management Studio. However, you should perform these tasks in either Symantec Endpoint Protection Manager or Management Studio, but not both. See the knowledge base article: Create database maintenance plans in MS SQL Server 2005 using SQL Server Integration Services (SSIS).

To run database maintenance tasks on demand

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

2   Under **Servers**, click the icon that represents the database.

3   Under **Tasks**, select either of the following options:

- **Truncate Transaction Log Now**

- **Rebuild Indexes Now**

4   Click **Run**.

5   After the task completes, click **Close**.

To schedule database maintenance tasks to run automatically

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

2   Under **Servers**, click the icon that represents the database.

3   Under **Tasks**, click **Edit Database Properties**.

4   On the **General** tab, check either or both of the following options, then click **Schedule Task** and specify the schedule for each task.

   ■   **Truncate the database transaction logs**. The default schedule for this task is every four hours.

   ■   **Rebuild Indexes**. The default schedule for this task is every Sunday at 2:00.

Warning: If you perform these tasks in SQL Server Management Studio, uncheck these options.

See "Scheduling automatic database backups" on page 725.

Increasing the Microsoft SQL Server database file size

If you use the Microsoft SQL Server database, periodically check the database size to make sure that the database does not reach its maximum size. If you can, increase the maximum size that the Microsoft SQL Server database holds.

See "Scheduling automatic database maintenance tasks" on page 726.

To increase the Microsoft SQL Server database size

1   On the management server, locate the installation path for Microsoft SQL Server.

   The default path is:

   `C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data.`

2   Expand the Data folder, right-click **sem5**, and click **Properties**.

3   In the **Database Properties** dialog box, select **Files**.

4   Under **Database files**, select **sem5_log1**, and scroll to the right to view the **Autogrowth** column.

5   In the **Autogrowth** column, click the **...** button.

6 In the **Change Autogrowth for** *sem5_log1* dialog box, click **Unrestricted File Growth**, and then click **OK**.

7 Click **OK**.

Exporting data to a Syslog server

To increase the space in the database, you can configure the management server to send the log data to a Syslog server.

When you export log data to a Syslog server, you must configure the Syslog server to receive the logs.

See "Exporting log data to a text file" on page 729.

To export log data to a Syslog server

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

2 Click **Servers**.

3 Click the local site or remote site that you want to export log data from.

4 Click **Configure External Logging**.

5 On the **General** tab, in the **Update Frequency** list box, select how often to send the log data to the file.

6 In the **Master Logging Server** list box, select the management server to send the logs to.

   If you use SQL Server and connect multiple management servers to the database, specify only one server as the Master Logging Server.

7 Check **Enable Transmission of Logs to a Syslog Server**.

8 Provide the following information:

   ■ **Syslog Server**
   Type the IP address or domain name of the Syslog server that you want to receive the log data.

   ■ **Destination Port**
   Select the protocol to use, and type the destination port that the Syslog server uses to listen for Syslog messages.

   ■ **Log Facility**
   Type the number of the log facility that you want to the Syslog configuration file to use, or use the default. Valid values range from 0 to 23.

9 On the **Log Filter** tab, check which logs to export.

10 Click **OK**.

Exporting log data to a text file

When you export data from the logs to a text file, by default the files are placed in a folder. That folder path is *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\dump. Entries are placed in a .tmp file until the records are transferred to the text file.

If you do not have Symantec Network Access Control installed, some of these logs do not exist.

Note: You cannot restore the database by using exported log data.

Table 34-2 shows the correspondence of the types of log data to the names of the exported log data files. The log names do not correspond one-to-one to the log names that are used on the **Logs** tab of the **Monitors** page.

Table 34-2   Log text file names for Symantec Endpoint Protection

Log Data	Text File Name
Server Administration	scm_admin.log
Application and Device Control	agt_behavior.log
Server Client	scm_agent_act.log
Server Policy	scm_policy.log
Server System	scm_system.log
Client Packet	agt_packet.log
Client Proactive Threat	agt_proactive.log
Client Risk	agt_risk.log
Client Scan	agt_scan.log
Client Security	agt_security.log
Client System	agt_system.log
Client Traffic	agt_traffic.log

Table 34-3 shows the correspondence of the types of log data to the names of the exported log data files for the **Enforcer** logs.

Table 34-3   Log text file names for the Enforcer logs

Log Data	Text File Name
Server Enforcer Activity	scm_enforcer_act.log
Enforcer Client Activity	enf_client_act.log
Enforcer System	enf_system.log
Enforcer Traffic	enf_traffic.log

Note: When you export to a text file, the number of exported records can differ from the number that you set in the **External Logging** dialog box. This situation arises when you restart the management server. After you restart the management server, the log entry count resets to zero, but there may already be entries in the temporary log files. In this situation, the first *.log file of each type that is generated after the restart contains more entries than the specified value. Any log files that are subsequently exported contain the correct number of entries.

To export log data to a text file

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

2   Click **Servers**.

3   Click the local site or remote site that you want to configure external logging for.

4   Click **Configure External Logging**.

5   On the **General** tab, select how often you want the log data to be sent to the file.

6   In the **Master Logging Server** list box, select the server that you want to send logs to.

    If you use Microsoft SQL with more than one management server connecting to the database, only one server needs to be a Master Logging Server.

7   Check **Export Logs to a Dump File**.

8   If necessary, check **Limit Dump File Records** and type in the number of entries that you want to send at a time to the text file.

9   On the **Log Filter** tab, select all of the logs that you want to send to text files.

If a log type that you select lets you select the severity level, you must check the severity levels that you want to export.

10   Click **OK**.

Exporting log data to a comma-delimited text file

You can export the data in the logs to a comma-delimited text file.

See "Exporting data to a Syslog server" on page 728.

To export logs to a comma-delimited text file

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

2   On the **Logs** tab, select the log that you want to export.

3   Click **View Log**.

4   Click **Export**.

5   In **File Download** dialog box, click **Save**.

6   Specify the file name and location, and then click **Save**.

7   Click **Close**.

Specifying client log size and which logs to upload to the management server

Company policy might require you to increase the time and type of log events that the database keeps. You can specify the number of entries kept in the logs and the number of days that each entry is kept on the client.

You can configure whether or not to upload each type of client log to the server, and the maximum size of the uploads. If you choose not to upload the client logs, it has the following consequences:

■   You cannot view the client log data from the Symantec Endpoint Protection Manager console by using the **Logs** tab on the **Monitors** page.

■   You cannot back up the client logs when you back up the database.

■   You cannot export the client log data to a file or a centralized log server.

> **Note:** Some client log settings are group-specific and some are set in the Virus and Spyware Protection policy, which can be applied to a location. If you want all remote client log and office client log settings to differ, you must use groups instead of locations to manage remote clients.

See "Specifying how long to keep log entries in the database" on page 732.

To specify client log size and which logs to upload to the management server

1   On the console, click **Clients**, and select a group.

2   On the **Policies** tab, under **Location-independent Policies and Settings**, click **Client Log Settings**.

3   In the **Client Log Settings** for *group name* dialog box, set the maximum file size and the number of days to keep log entries.

4   Check **Upload to management server** for any logs that you want the clients to forward to the server.

5   For the **Security** log and **Traffic** log, set the damper period and the damper idle period.

    These settings determine how frequently **Network Threat Protection** events are aggregated.

6   Click **OK**.

Specifying how long to keep log entries in the database

To help control hard disk space, you can decrease the number of log entries that the database keeps. You can also configure the number of days the entries are kept.

> **Note:** Log information on the Symantec Endpoint Protection Manager console **Logs** tab on the **Monitors** page is presented in logical groups for you to view. The log names on the **Site Properties Log Settings** tab correspond to log content rather than to log types on the **Monitors** page **Logs** tab.

See "Specifying client log size and which logs to upload to the management server" on page 731.

To specify how long to keep log entries in the database

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

2   Under **Servers**, expand **Local Site**, and click the database.

3   Under **Tasks**, click **Edit Database Properties**.

4   On the **Log Settings** tab, set the number of entries and number of days to keep log entries for each type of log.

5   Click **OK**.

About increasing the disk space on the server for client log data

A configuration that uploads a large volume of client log data to the server at frequent intervals can cause disk space problems on the server. If you must upload a large volume of client log data, you may have to adjust some default values to avoid these space problems. As you deploy to clients, you should monitor the space on the server in the log insertion directory and adjust these values as needed.

The default directory where the logs are converted to .dat files and then written to the database is in the following location:

drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\
data\inbox\log.

To adjust the values that control the space available on the server, you must change these values in the Windows registry. The Windows registry keys that you need to change are located on the server in HKEY_LOCAL_MACHINE\
SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM.

Table 34-4 lists the Windows registry keys and their default values and describes what they do.

Table 34-4   Windows registry keys that contain log upload settings

Value name	Description
MaxInboxSpace	Specifies the space that is allotted for the directory where log files are converted to .dat files before they are stored in the database. The default value is 8 GB.

Table 34-4	Windows registry keys that contain log upload settings *(continued)*
Value name	**Description**
`MinDataFreeSpace`	Specifies the minimum amount of space that should be kept free in this directory. This key is useful to ensure that other applications that use the same directory have enough space to run without an adverse effect on performance. The default value is 200 MB.
`IntervalOfInboxSpaceChecking`	Specifies how long the management server waits before it checks on the amount of space in the inbox that is available for log data. The default value is 30 seconds.

See "Maintaining the database" on page 721.

Clearing log data from the database manually

You can perform a manual log sweep after backing up the database, if you prefer to use this method as part of routine database maintenance.

If you allow an automatic sweep to occur, you may lose some log data if your database backups do not occur frequently enough. If you regularly perform a manual log sweep after you have performed a database backup, it ensures that you retain all your log data. This procedure is very useful if you must retain your logs for a relatively long period of time, such as a year. You can manually clear the logs, but this procedure is optional and you do not have to do it.

See "Backing up the database and logs" on page 744.

See "Specifying how long to keep log entries in the database" on page 732.

To clear log data from the database manually

1   To prevent an automatic sweep of the database until after a backup occurs, increase a site's log size to their maximums.

2   Perform the backup, as appropriate.

3   On the computer where the manager is installed, open a Web browser and type the following URL:

https://localhost:8443/servlet/ConsoleServlet?ActionType=ConfigServer&action =SweepLogs

After you have performed this task, the log entries for all types of logs are saved in the alternate database table. The original table is kept until the next sweep is initiated.

4   To empty all but the most current entries, perform a second sweep. The original table is cleared and entries then start to be stored there again.

5   Return the settings on the **Log Settings** tab of the **Site Properties** dialog box to your preferred settings.

Managing failover and load balancing

This chapter includes the following topics:

- Setting up failover and load balancing

- About failover and load balancing

- Configuring a management server list

- Assigning a management server list to a group and location

Setting up failover and load balancing

The client computers must be able to connect to a management server at all times to download the security policy and to receive log events.

Failover is used to maintain communication with a Symantec Endpoint Protection Manager when the management server becomes unavailable. Load balancing is used to distribute client management between multiple management servers.

You can set up failover and load balancing if you use a Microsoft SQL Server database. You can set up failover with the embedded database, but only if you use replication. When you use replication with an embedded database, Symantec recommends that you do not configure load balancing, as data inconsistency and loss may result.

To set up failover and load balancing, you add multiple management servers or Enforcers to a management server list.

Table 35-1 lists the tasks that you should perform to set up failover and load balancing.

Table 35-1   Process for setting up failover and load balancing

Tasks	Description
Read about failover and load balancing.	You should understand if and when you need to set up a failover and load balancing configurations. See "About failover and load balancing" on page 738.
Add management servers to a management server list.	You can either use the default management server list or add management servers to a new management server list. A management server list includes the IP addresses or host names of management servers to which clients and Enforcers can connect. See "Configuring a management server list" on page 740.
Assign the custom management server list to a group.	After you have created a custom management server list, you must assign the management server list to a group. See "Assigning a management server list to a group and location" on page 741.
Fix communication problems with the management server.	If the management server goes offline, or the client and the management server do not communicate, you should also troubleshoot the problem. See "Troubleshooting communication problems between the management server and the client" on page 756.

See "Setting up sites and replication" on page 187.

About failover and load balancing

You can install two or more management servers that communicate with one Microsoft SQL Server database and configure them for failover or load balancing. Since you can install only one Symantec Endpoint Protection Manager to communicate with the embedded database, you can set up failover only if you replicate with another site. When you use replication with an embedded database, Symantec recommends that you do not configure load balancing, as data inconsistency and loss may result.

A management server list is a prioritized list of management servers that is assigned to a group. You should add at least two management servers to a site to automatically distribute the load among them. You can install more management servers than are required to handle your clients to protect against the failure of an individual management server. In a custom management server list, each server is assigned to a priority level. A client that comes onto the network selects a priority one server to connect to at random. If the first server it tries is

unavailable and there are other priority one servers in the list, it randomly tries to connect to another. If no priority one servers are available, then the client tries to connect to one of the priority two servers in the list. This method of distributing client connections randomly distributes the client load among your management servers.

Figure 35-1 shows components on different subnets. Management servers and database servers can be on the same subnets. The servers are identified with the numbers 1 and 2, which signify a failover configuration.

Figure 35-1   Failover configuration
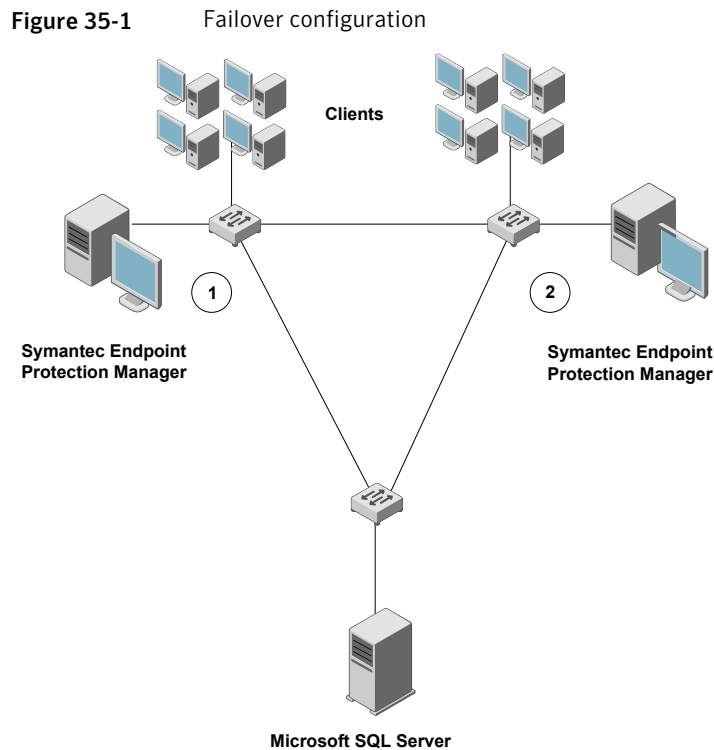
In a failover configuration, all clients send traffic to and receive traffic from server 1. If server 1 goes offline, all clients send traffic to and receive traffic from server 2 until server 1 comes back online. The database is illustrated as a remote installation, but it also can be installed on a computer that runs the Symantec Endpoint Protection Manager.

You may also want to consider failover for content updates, if you intend to use local servers. All the components that run LiveUpdate can also use a prioritized list of update sources. Your management servers can use a local LiveUpdate server and failover to LiveUpdate servers in other physical locations.

> **Note:** The use of internal LiveUpdate servers, Group Update Providers, and site replication does not provide load balancing functionality. You should not set up multiple sites for load balancing.

See "Configuring a management server list" on page 740.

See "About determining how many sites you need" on page 189.

See "Setting up sites and replication" on page 187.

See "Setting up failover and load balancing" on page 737.

Configuring a management server list

By default, the management servers are assigned the same priority when configured for failover and load balancing. If you want to change the default priority after installation, you can do so by using the Symantec Endpoint Protection Manager console. Failover and load balancing can be configured only when a site includes more than one management server.

To provide both load balancing and roaming:

- Enable DNS and put a domain name as the only entry in a custom management server list.

- Enable the Symantec Endpoint Protection location awareness feature and use a custom management server list for each location. Create at least one location for each of your sites.

- Use a hardware device that provides failover or load balancing. Many of these devices also offer a setup for roaming.

See "About failover and load balancing" on page 738.

To configure a management server list

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

2   Expand **Policy Components**, and then click **Management Server Lists**.

3   Under **Tasks**, click **Add a Management Server List.**

4   In the **Management Server Lists** dialog box, click **Add > New Server**.

5   In the **Add Management Server** dialog box, in the **Server Address** box, type the fully qualified domain name or IP address of a management server or Enforcer.

    If you type an IP address, be sure that it is static, and that all clients can resolve it.

6 Click **OK**.

7 Add any additional servers.

8 To configure load balancing with another management server, click **Add > New Priority**.

9 To change the priority of a server for load balancing, select a server, and then do one of the following tasks:

■ To get clients to connect to that particular server first, click **Move Up**.

■ To give a server lower priority, click **Move Down**.

10 Click **OK**.

You must then apply the management server list to a group.

See "Assigning a management server list to a group and location" on page 741.

Assigning a management server list to a group and location

After you add a policy, you must assign it to a group or a location or both. You can also use the management server list to move a group of clients from one management server to another.

You must have finished adding or editing a management server list before you can assign the list.

See "Configuring a management server list" on page 740.

To assign a management server list to a group and location

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

2 In the **Policies** page, expand **Policy Components**, and then click **Management Server Lists**.

3 In the **Management Server Lists** pane, select the management server list you want to assign.

4 Under **Tasks**, click **Assign the List**.

5 In the **Apply Management Server List** dialog box, check the groups and locations to which you want to apply the management server list.

6 Click **Assign**.

7 Click **Yes**.

To assign a management server list to a group or location on the Clients page

1   In the console, click **Clients > Policies**

2   On the **Policies** tab, select the group, and then uncheck **Inherit policies and settings from parent group**.

    You cannot set any communication settings for a group unless the group no longer inherits any policies and settings from a parent group.

3   Under **Location-independent Policies and Settings**, click **Communication Settings**.

4   In the **Communication Settings for *group name*** dialog box, under **Management Server List**, select the management server list.

    The group that you select then uses this management server list when communicating with the management server.

5   Click **OK**.

Preparing for disaster recovery

This chapter includes the following topics:

-
-
-

Preparing for disaster recovery

In case of hardware failure or database corruption, you should back up the information that is collected after you install Symantec Endpoint Protection Manager. You then copy these files to another computer.

Table 36-1 High-level steps to prepare for disaster recovery

Step	Action	Description
Step 1	Back up the database	Back up the database regularly, preferably weekly.
		By default, the database backup folder is saved to the following location:
		Drive: `\\Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup`.
		The backup file is called *date_timestamp*.zip.
		See "Backing up the database and logs" on page 744.

	Table 36-1	High-level steps to prepare for disaster recovery *(continued)*

Step	Action	Description
Step 2	Back up the disaster recovery file Update or back up the server certificate (optional)	The recovery file includes the encryption password, keystore files domain ID, certificate files, license files, and port numbers. By default, the file is located in the following directory: `Drive:\\Program Files\Symantec\ Symantec Endpoint Protection Manager\Server Private Key Backup\recovery_timestamp.zip` **Note:** The recovery file only stores the default domain ID. If you have multiple domains, the recovery file does not store that information. If you need to perform disaster recovery, you must re-add the domains. See "Adding a domain" on page 267. If you update the self-signed certificate to a different certificate type, the management server creates a new recovery file. Because the recovery file has a timestamp, you can tell which file is the latest one. See "Updating or restoring a server certificate" on page 713. See "Backing up a server certificate" on page 746.
Step 3	Save the IP address and host name of the management server to a text file (optional)	If you have a catastrophic hardware failure, you must reinstall the management server using the IP address and host name of the original management server. Add the IP address and host name to a text file, such as: `Backup.txt`.
Step 4	Copy the files you backed up in the previous steps to another computer	Copy the backed up files to a computer in a secure location.

See "Performing disaster recovery" on page 749.

See "Backing up your license files" on page 121.

See the knowledge base article Best Practices for Disaster Recovery with the Symantec Endpoint Protection Manager.

See "Exporting and importing server settings" on page 719.

Backing up the database and logs

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

By default, the backup file is saved in the following folder: `Drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\backup`.

The backups are placed in a .zip file. By default, the backup database file is named *date_timestamp*.zip, the date on which the backup occurs.

Note: Avoid saving the backup file in the product installation directory. Otherwise, the backup file is removed when the product is uninstalled.

Log data is not backed up unless you configure Symantec Endpoint Protection Manager to back it up. If you do not back up the logs, then only your log configuration options are saved during a backup. You can use the backup to restore your database, but the logs in the database are empty of data when they are restored.

You can keep up to 10 versions of site backups. You should ensure that you have adequate disk space to keep all your data if you choose to keep multiple versions.

The database backup might take several minutes to complete. You can check the System log as well as the backup folder for the status during and after the backup.

You can back up the database immediately, or schedule the backup to occur automatically. You can back up an embedded database or a Microsoft SQL Server database that is configured as the Symantec Endpoint Protection Manager database.

See "Scheduling automatic database backups" on page 725.

See "Preparing for disaster recovery" on page 743.

To back up the database and logs

1   On the computer that runs Symantec Endpoint Protection Manager, on the **Start** menu, click **All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools > Database Back Up and Restore**.

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

3   In the **Back Up Database** dialog box, optionally check **Backup logs**, and then click **Yes**.

4   Click **OK**.

5   When the database backup completes, click **Exit**.

6   Copy the backup database file to another computer.

To back up the database and logs from within the console

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

2   Under **Servers**, click the icon that represents the database.

3   Under **Tasks**, click **Back Up Database Now**.

4   In the **Back Up Database** dialog box, optionally check **Backup logs**, and then click **Yes**.

5   Click **OK**.

6   Click **Close**.

Backing up a server certificate

In case the computer on which the management server is installed gets corrupted, you should back up the private key and the certificate.

The JKS Keystore file is backed up during the initial installation. A file that is called server_*timestamp*.xml is also backed up. The JKS Keystore file includes the server's private and public key pair and the self-signed certificate.

To back up a server certificate

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

2   Under **Servers**, click the management server whose server certificate you want to back up.

3   Under **Tasks**, click **Manage Server Certificate**, and then click **Next**.

4   In the **Manage Server Certificate** panel, click **Back up the server certificate** and then click **Next**.

5   In the **Back Up Server Certificate** panel, click **Browse** to specify a backup folder, and then click **Open**.

     Note that you back up the management server certificate into the same folder.

6   In the **Backup Server Certificate** panel, click **Next**.

7   Click **Finish**.

See "About server certificates" on page 709.

Section

6

Troubleshooting Symantec Endpoint Protection

Performing disaster recovery

This chapter includes the following topics:

- Performing disaster recovery

- Reinstalling or reconfiguring Symantec Endpoint Protection Manager

- Generating a new server certificate

- Restoring the database

Performing disaster recovery

Table 37-1 lists the steps to recover your Symantec Endpoint Protection environment in the event of hardware failure or database corruption.

Note: This topic assumes that you have prepared for disaster recovery and have created backups and recovery files.

Table 37-1   Process for performing disaster recovery

Step	Action
Step 1	Reinstall Symantec Endpoint Protection Manager using a disaster recovery file.
	By reinstalling the management server, you can recover the files that were saved after initial installation.
	See "Reinstalling or reconfiguring Symantec Endpoint Protection Manager" on page 750.
	If you reinstall Symantec Endpoint Protection Manager on a different computer and without using the disaster recovery file, you must generate a new server certificate.
	See "Generating a new server certificate" on page 751.
Step 2	Restore the database.
	See "Restoring the database" on page 752.

See "Preparing for disaster recovery" on page 743.

See the knowledge base article: Perform a disaster recovery when the database backup/restore process fails using the "Database Backup/Restore Wizard" for an Embedded Database.

Reinstalling or reconfiguring Symantec Endpoint Protection Manager

If you need to reinstall or reconfigure the management server, you can import all your settings by using a disaster recovery file. You can reinstall the software on the same computer, in the same installation directory.

You can also use this procedure to install an additional site for replication.

The Symantec Endpoint Protection Manager creates a recovery file during installation. The recovery file is selected by default during the reinstallation process.

See "Preparing for disaster recovery" on page 743.

To reinstall the management server

1   Uninstall the existing management server.

2   Install the server from the product disc.

    See "Installing Symantec Endpoint Protection Manager" on page 95.

3 In the **Welcome** panel, make sure that the **Use a recovery file** option is checked, and then click **Next**.

By default, the recovery file is located in: `Drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup`.

4 Follow the instructions in each panel. The default settings work for most cases. If the reinstalled server connects to an existing database, you change the database settings to those of the existing database.

You can also restore the database if necessary. However, if the Symantec Endpoint Protection Manager database is hosted on another computer or is otherwise not affected, you do not need to restore your database.

See "Restoring the database" on page 752.

To reconfigure the management server

1 To reconfigure the management server, click **Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools > Management Server Configuration Wizard**.

2 To install a management server for replication, click **Install an additional site**.

3 Follow the instructions in each panel.

Generating a new server certificate

If you reinstall Symantec Endpoint Protection Manager on a different computer, you must generate a new server certificate.

If the original computer is corrupted or you upgrade the management server from a previous version, you must reinstall Symantec Endpoint Protection Manager on a different computer. To reinstall Symantec Endpoint Protection Manager on a different computer, you install the management server as if for the first time, rather than with the recovery file.

You reinstall the database settings on a different computer by using the database backup and restore utility. However, the server certificate that the new management server uses does not match the existing server certificate in the restored database. Because client-server communication uses the server certificate, you must generate a new server certificate.

See "Reinstalling or reconfiguring Symantec Endpoint Protection Manager" on page 750.

See "Installing Symantec Endpoint Protection Manager" on page 95.

To generate a new server certificate

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

2   Under **Servers**, click the management server.

3   Under **Tasks**, click **Manage Server Certificate**, and then click **Next**.

4   In the **Manage Server Certificate** panel, click **Generate new server certificate** and then click **Next**.

5   Click **Yes**, and then click **Next**.

After you log on to Symantec Endpoint Protection Manager, you are asked to trust the new certificate.

See "Logging on to the Symantec Endpoint Protection Manager console" on page 99.

Restoring the database

If the database gets corrupted or you need to perform disaster recovery, you can restore the database. To restore the database, you must first have backed it up.

See "Backing up the database and logs" on page 744.

You must restore the database using the same version of Symantec Endpoint Protection Manager that you used to back up the database. You can restore the database on the same computer on which it was installed originally or on a different computer.

The database restore might take several minutes to complete.

To restore the database

1   Stop the management server service.

    See "Stopping and starting the management server service" on page 170.

2   On the **Start** menu, click **All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools > Database Back Up and Restore**.

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

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

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

    Locate the copy of the backup database file that you made when you backed up the database. By default, the backup database file is named *date_timestamp*.zip.

6 Click **OK**.

7 Click **Exit**.

8 Restart the management server service.

Troubleshooting installation and communication problems

This chapter includes the following topics:

- Troubleshooting computer issues with the Symantec Help support tool
- Identifying the point of failure of an installation
- Troubleshooting communication problems between the management server and the client
- Troubleshooting communication problems between the management server and the console or the database
- Client and server communication files

Troubleshooting computer issues with the Symantec Help support tool

You can download a utility to diagnose common issues you encounter with installing and using Symantec Endpoint Protection Manager or the Symantec Endpoint Protection client.

The support tool helps you with the following issues:

- Lets you quickly and accurately identify known issues.
- When the tool recognizes an issue, the tool redirects you to the resources to resolve the issue yourself.

■ When an issue is not resolved, the tool lets you easily submit data to Support for further diagnostics.

To troubleshoot computer issues with the Symantec Help support tool

1   Do one of the following tasks:

   ■ See the knowledge base article: Symantec Help (SymHelp)

   ■ In the client, click **Help > Download Support Tool**

2   Follow the on-screen instructions.

Identifying the point of failure of an installation

The Windows Installer and Push Deployment Wizard create log files that can be used to verify whether or not an installation was successful. The log files list the components that were successfully installed and provide a variety of details that are related to the installation package. You can use the log file to help identify the component or the action that caused an installation to fail. If you cannot determine the reason for the failed installation, you should retain the log file. Provide the file to Symantec Technical Support if it is requested.

Note: Each time the installation package is executed, the log file is overwritten.

To identify the point of failure of an installation

1   In a text editor, open the log file that the installation generated.

2   To find failures, search for the following entry:

```
Value 3
```

The action that occurred before the line that contains this entry is most likely the action that caused the failure. The lines that appear after this entry are the installation components that have been rolled back because the installation was unsuccessful.

Troubleshooting communication problems between the management server and the client

If you have trouble with client and server communication, you should first check to make sure that there are no network problems. You should also check network connectivity before you call Symantec Technical Support.

You can test the communication between the client and the management server in several ways.

Table 38-1 Checking the connection between the management server and the client

What to check	Solution
Look on the client to see if the client connects to the management server	You can download and view the troubleshooting file on the client to verify the communication settings.
	See "How to determine whether the client is connected and protected" on page 697.
	See "Checking the connection to the management server on the client computer" on page 759.
	See "Investigating protection problems using the troubleshooting file on the client" on page 760.
Test the connectivity between the client and the management server	You can perform several tasks to check the connectivity between the client and the management server.
	■ See "Enabling and viewing the Access log to check whether the client connects to the management server" on page 760.
	■ Ping the management server from the client computer. See "Using the ping command to test the connectivity to the management server" on page 762.
	■ Use a Web browser on the client computer to connect to the management server. See "Using a browser to test the connectivity to Symantec Endpoint Protection Manager on the Symantec Endpoint Protection client" on page 762.

Table 38-1 Checking the connection between the management server and the client *(continued)*

What to check	Solution
Check that the management server uses the correct server certificate	If you reinstalled Symantec Endpoint Protection Manager, check that the correct server certificate was applied. If the management server uses a different server certificate, the server still downloads content, but the client cannot read the content.. If the management server uses the wrong server certificate, you must update it.
	See "Updating or restoring a server certificate" on page 713.
	See "Best practices for updating server certificates and maintaining the client-server connection" on page 710.
	You can verify that the management server uses the wrong server certificate by checking the following items:
	■ The client does not display the green dot in the taskbar, which indicates that it does not communicate with the management server. See "How to determine whether the client is connected in the console" on page 224. ■ The client does not receive policy updates from the management server. ■ The management server shows that it does connect with the client. See "How to determine whether the client is connected and protected" on page 697.
Check for any network problems	You should verify that there are no network problems by checking the following items:
	■ Test the connectivity between the client and the management server first. If the client computer cannot ping or Telnet to the management server, you should verify the DNS service for the client. ■ Check the client's routing path. ■ Check that the management server does not have a network problem. ■ Check that the Symantec Endpoint Protection firewall (or any third-party firewall) does not cause any network problems.

Table 38-1   Checking the connection between the management server and the
                    client *(continued)*

What to check	Solution
Check the debug logs on the client	You can use the debug log on the client to determine if the client has communication problems. See "Checking the debug log on the client computer" on page 763. See "Checking the inbox logs on the management server" on page 763.
Recover lost client communication	If the clients have lost the communication with a management server, you can use a tool to recover the communication file. See "Restoring client-server communication settings by using the SylinkDrop tool" on page 764.

If Symantec Endpoint Protection Manager displays logging errors or HTTP error
codes, see the following knowledge base article: Symantec Endpoint Protection
Manager communication troubleshooting.

Checking the connection to the management server on the client computer

If you have a managed client, you can check your connection to the management
server. If you are not connected to the management server, you can request that
your client connect.

See "Troubleshooting communication problems between the management server
and the client" on page 756.

Checking the connection to the management server on the client computer

1   On the **Status** page, click **Help > Troubleshooting**.

2   In the **Troubleshooting** dialog box, click **Connection Status**.

3   In the **Connection Status** pane, you can see the last attempted connection
    and the last successful connection.

4   To reestablish a connection with the management server, click **Connect Now**.

Investigating protection problems using the troubleshooting file on the client

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

Symantec Technical Support might request that you email the `Troubleshooting.txt` file.

See "Troubleshooting communication problems between the management server and the client" on page 756.

To export the troubleshooting file from the client

1   On the client computer, open the client.

2   In the client, click **Help** > **Troubleshooting**.

3   In the **Management** pane, under **Troubleshooting Data**, click **Export**.

4   In the **Save As** dialog box, accept the default troubleshooting file name or type a new file name, and then click **Save**.

    You can save the file on the desktop or in a folder of your choice.

5   Using a text editor, open `Troubleshooting.txt` to examine the contents.

Enabling and viewing the Access log to check whether the client connects to the management server

You can view the Apache HTTP server Access log on the management server to check whether the client connects to the management server. If the client connects, the client's connection problem is probably not a network issue. Network issues include the firewall blocking access, or networks not connecting to each other.

You must first enable the Apache HTTP server Access log before you can view the log.

Note: Disable the log after you view it because the log uses unnecessary CPU resources and hard disk space.

See "Troubleshooting communication problems between the management server and the client" on page 756.

To enable the Apache HTTP server Access log

1 In a text editor, open the file *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\apache\conf\httpd.conf.

2 In the httpd.conf file, remove the hash mark (#) from the following text string and then save the file:

```
#CustomLog "logs/access.log" combined
```

3 Stop and restart the Symantec Endpoint Protection Manager service and Apache HTTP server:

See "Stopping and starting the management server service" on page 170.

See "Stopping and starting the Apache Web server" on page 761.

To view the Apache HTTP server Access log

1 On the management server, open *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\apache\logs\access.log

2 Look for a client computer's IP address or host name, which indicates that clients connect to the Apache HTTP server.

3 Disable the Apache HTTP server Access log.

Stopping and starting the Apache Web server

When you install Symantec Endpoint Protection Manager, it installs the Apache Web server. The Apache Web server runs as an automatic service. You may need to stop and restart the Web server to enable the Apache HTTP Server Access log.

See "Enabling and viewing the Access log to check whether the client connects to the management server" on page 760.

To stop the Apache Web server

◆ From a command prompt, type:

```
net stop semwebsrv
```

To start the Apache Web server

◆ From a command prompt, type:

```
net start semwebsrv
```

Using the ping command to test the connectivity to the management server

You can try to ping the management server from the client computer to test connectivity.

See "Troubleshooting communication problems between the management server and the client" on page 756.

To use the ping command to test the connectivity to the management server

1   On the client, open a command prompt.

2   Type the ping command. For example:

    ping *name*

    where *name* is the computer name of the management server. You can use the server IP address in place of the computer name. In either case, the command should return the server's correct IP address.

    If the ping command does not return the correct address, verify the DNS service for the client and check its routing path.

Using a browser to test the connectivity to Symantec Endpoint Protection Manager on the Symantec Endpoint Protection client

You can use a Web browser on the client computer to test the connectivity between the management server and the client. This method helps determine if the client has a problem with the connection or network, or a problem with the client.

You can also check the connection between the management server on the client computer by using the following methods:

■   Checking whether the Symantec Endpoint Protection client status icon shows a green dot.
    See "How to determine whether the client is connected and protected" on page 697.

■   Checking the connection status on the Symantec Endpoint Protection client.
    See "Checking the connection to the management server on the client computer" on page 759.

To use a browser to test the connectivity to Symantec Endpoint Protection Manager on the Symantec Endpoint Protection client

1 On the client computer, open a Web browser, such as Internet Explorer.

2 In the browser command line, type the following command:

   http://*management server address*:8014/secars/secars.dll?hello,secars

   where *management server address* is the management server's DNS name, NetBios name, or IP address.

3 When the Web page appears, look for one of the following results:

   ■ If the word **OK** appears, the client computer connects to the management server. Check the client for a problem.

   ■ If the word **OK** does not appear, the client computer does not connect to the management server. Check the client's network connections and that network services are running on the client computer. Verify the DNS service for the client and check its routing path.
   See "Troubleshooting communication problems between the management server and the client" on page 756.

Checking the debug log on the client computer

You can check the debug log on the client. If the client has communication problems with the management server, status messages about the connection problem appear in the log.

See "Troubleshooting communication problems between the management server and the client" on page 756.

You can check the debug log by using the following methods:

■ In the client, on the Help and Support menu, in the Troubleshooting dialog box, you can click **Edit Debug Log Settings** and type a name for the log. You can then click **View Log**.

■ You can use the Windows registry to turn on debugging in the client.
   You can find the Windows registry key in the following location:
   HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\smc_debuglog_on

Checking the inbox logs on the management server

You can use a Windows registry key to generate logs about activity in the management server inbox. When you modify the Windows registry key, the

management server generates the logs (ersecreg.log and exsecars.log). You can view these logs to troubleshoot client and server communication.

See "Troubleshooting communication problems between the management server and the client" on page 756.

See "Checking the debug log on the client computer" on page 763.

To check the inbox logs on the management server

1   On the management server, under HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM, set the DebugLevel value to 3.

     Typically, the inbox appears in the following location on the management server computer:

```
\Program Files\Symantec\Symantec Endpoint Protection Manager\data\
inbox\log
```

2   Open the log with Notepad.

Restoring client-server communication settings by using the SylinkDrop tool

The Sylink.xml file includes communication settings between the client and a Symantec Endpoint Protection Manager server. If the clients have lost the communication with a management server, you must replace the old Sylink.xml file with a new Sylink.xml file. The SylinkDrop tool automatically replaces the Sylink.xml file on the client computer with a new Sylink.xml file.

Note: You can also replace the Sylink.xml file by redeploying a client installation package. Use this method for a large number of computers, for computers that you cannot physically access easily or computers that require administrative access.See "Restoring client-server communications by using a client installation package" on page 701.

When you run the SylinkDrop tool, it can also perform the following tasks:

■ Migrates or moves clients to a new domain or management server.

■ Restores the communication breakages to the client that cannot be corrected on the management server.

■ Moves a client from one server to another server that is not a replication partner.

■ Moves a client from one domain to another.

- Converts an unmanaged client to a managed client.

- Converts a managed client to an unmanaged client.

You can write a script with the tool to modify communication settings for large numbers of clients.

See "About managed and unmanaged clients" on page 146.

See "Troubleshooting communication problems between the management server and the client" on page 756.

Note: You must disable Tamper Protection to use the SylinkDrop.exe tool. You can also create a Tamper Protection exception for the SylinkDrop.exe tool.

See "Changing Tamper Protection settings" on page 412.

See "Creating a Tamper Protection exception" on page 539.

To recover client-server communication settings by using the SylinkDrop tool

1   In the console, export the communications file from the group that connects to the management server to which you want the client computer to connect. The communications file is the Sylink.xml file.

See "Exporting the client-server communications file manually" on page 702.

2   Copy the communication file to the client computer.

You can either save the file to a network location, email it to the user on the client computer, or copy it to removable media.

3   Do one of the following tasks:

- On the tools product disc, locate `\Tools\SylinkDrop\SylinkDrop.exe`.

- On the computer that runs the management server, locate *drive*:`\Program Files (x86)\Symantec\Symantec Endpoint Protection\`*Version.Number*`\Bin\SylinkDrop.exe`

You can run the tool remotely or save it and then run it on the client computer. If you use the tool on the command line, read the SylinkDrop.txt file for a list of the tool's command parameters.

4   In the **Sylink Drop** dialog box, click **Browse**, and locate the .xml file you deployed in step 2 to the client computer.

5   Click **Update Sylink**.

6   When you see a confirmation dialog box, click **OK**.

7   In the **Sylink Drop** dialog box, click **Exit**.

Troubleshooting communication problems between the management server and the console or the database

If you have a connection problem with the console or the database, you may see one of the following symptoms:

- The management server service (semsrv) stops.

- The management server service does not stay in a started state.

- The Home, Monitors, and Reports pages display an HTTP error.

- The Home, Monitors, and Reports pages are blank.

- The Home, Monitors, and Reports pages display a continuously loading progress bar, without displaying any content.

All of these issues display a Java -1 error in the Windows Event log. To find the specific cause for the Java -1 error, look in the scm-server log. The scm-server log is typically located in the following location:

C:\Program Files\Symantec\Symantec Endpoint Protection Manager\tomcat\logs\scm-server-0.log

Table 38-2   Checking the communication with the console or database

What to check	Description
Test the connectivity between the database and the management server.	You can verify that the management server and the database communicate properly. See "Verifying the connection with the database" on page 767.
Check that the management server heap size is correct.	You may need to adjust the heap size that is appropriate for the management server's operating system. If you cannot log in to the management server's remote console, or if you see an out-of-memory message in the scm-server log, you may need to increase the heap size. The default heap size for Symantec Endpoint Protection Manager is 256 MB.
Check that the management server is not running multiple versions of PHP.	You can check whether the management server runs multiple software packages that use different versions of PHP. PHP checks for a global configuration file (php.ini). If there are multiple configuration files, you must force each product to use its own interpreter. When each product uses the correct version of PHP associated with it, the management server operates properly.

Table 38-2   Checking the communication with the console or database
                  (continued)

What to check	Description
Check the system requirements.	You can check whether both the client and the management server run the minimum or the recommended system requirements. For the most current system requirements, see: Release Notes and System Requirements for all versions of Symantec Endpoint Protection and Symantec Network Access Control

Verifying the connection with the database

The management server and the database may not communicate properly. You should verify that the database runs and then test the connection between the server and the database.

If the management server runs the embedded Sybase database, perform the following steps:

■   Verify that the Symantec Embedded Database service runs and that the dbsrv9.exe process listens to TCP port 2638.

■   Test the ODBC connection.

If the management server runs the remote SQL database, perform the following actions:

■   Verify that you have specified a named instance when you installed and configured Symantec Endpoint Protection Manager.

■   Verify that SQL Server runs and is properly configured.

■   Verify that the network connection between management server and the SQL database is correct.

■   Test the ODBC connection.

To verify communication with the embedded database

1   On the management server, click **Start > Control Panel > Administrative Tools**.

2   In the Administrative Tools dialog box, double-click **Data Sources (ODBC)**.

3   In the ODBC Data Source Administrator dialog box, click **System DSN**.

4   On the System DSN tab, double-click **SymantecEndpointSecurityDSN**.

5   On the ODBC tab, verify that the Data source name drop-down list is `SymantecEndpointSecurityDSN` and type an optional description.

6   Click **Login**.

7   On the Login tab, in the User ID text box, type `dba`.

8   In the Password text box, type the password for the database.

   This password is the one that you entered for the database when you installed the management server.

9   Click **Database**.

10   On the Database tab, in the Server name text box, type
    <*servername\instancename*>.

   If you use the English version of Symantec Endpoint Protection Manager, type the default, `sem5`. Otherwise, leave the Server name text box blank.

11   On the ODBC tab, click **Test Connection** and verify that it succeeds.

12   Click **OK**.

13   Click **OK**.

To verify communication to the SQL database

1   On the management server, click **Start > Control Panel > Administrative Tools**.

2   In the Administrative Tools dialog box, double-click **Data Sources (ODBC)**.

3   In the ODBC Data Source Administrator dialog box, click **System DSN**.

4   On the System DSN tab, double-click **SymantecEndpointSecurityDSN**.

5   In the Server drop-down list, verify that the correct server and instance is selected.

6   Click **Next**.

7   For Login ID, type `sa`.

8   In the Password text box, type the password for the database.

   This password is the one that you entered for the database when you installed the management server.

9   Click **Next** and make sure that `sem5` is selected for the default database.

10   Click **Next**.

11 Click **Finish**.

12 Click **Test Data Source** and look for the result that states:

```
TESTS COMPLETED SUCCESSFULLY!
```

Client and server communication files

The communication settings between the client and server and other client settings are stored in files on the client computer.

Table 38-3   Client files

File name	Description
SerDef.dat	An encrypted file that stores communication settings by location. Each time the user changes locations, the SerDef.dat file is read and the appropriate communication settings for the new location are applied to the client.
sylink.xml	Stores the global communication settings. This file is for internal use only and should not be edited. It contains settings from the Symantec Endpoint Protection Manager. If you edit this file, most settings will be overwritten by the settings from the management server the next time the client connects to the management server.
SerState.dat	An encrypted file that stores information about the user interface, such as the client's screen size, whether the client's console for Network Threat Protection appears, and whether Windows services appear. When the client starts, it reads this file and returns to the same user interface state as before it was stopped.

Troubleshooting reporting issues

This chapter includes the following topics:

- Troubleshooting reporting issues
- Changing timeout parameters for reviewing reports and logs
- Accessing reporting pages when the use of loopback addresses is disabled
- About recovering a corrupted client System Log on 64-bit computers

Troubleshooting reporting issues

You should be aware of the following information when you use reports:

- Timestamps, including client scan times, in reports and logs are given in the user's local time. The reporting database contains events in Greenwich Mean Time (GMT). When you create a report, the GMT values are converted to the local time of the computer on which you view the reports.

- If managed clients are in a different time zone from the management server, and you use the **Set specific dates** filter option, you may see unexpected results The accuracy of the data and the time on both the client and the management server may be affected.

- If you change the time zone on the server, log off of the console and log on again to see accurate times in logs and reports.

- In some cases, the report data does not have a one-to-one correspondence with what appears in your security products. This lack of correspondence occurs because the reporting software aggregates security events.

■ You can use SSL with the reporting functions for increased security. SSL
provides confidentiality, the integrity of your data, and authentication between
the client and the server.
See the knowledge base article: Configuring Secure Sockets Layer (SSL) to work
with the Symantec Endpoint Protection reporting functions on Windows Server
2003.

■ Risk category information in the reports is obtained from the Symantec
Security Response Web site. Until the Symantec Endpoint Protection Manager
console is able to retrieve this information, any reports that you generate show
Unknown in the risk category fields.

■ The reports that you generate give an accurate picture of compromised
computers in your network. Reports are based on log data, not the Windows
registry data.

■ If you get database errors when you run a report that includes a large amount
of data, you might want to change database timeout parameters.
See "Changing timeout parameters for reviewing reports and logs" on page 773.

■ If you get CGI or terminated process errors, you might want to change other
timeout parameters.
For more information, see the following document in the knowledge base
article: SAV Reporting Server or SEPM Reporting does not respond or shows
a timeout error message when querying large amounts of data.

■ If you have disabled the use of loopback addresses on the computer, the
reporting pages do not display.
See "Accessing reporting pages when the use of loopback addresses is disabled"
on page 774.

The following information is important to note if you have computers in your
network that are running legacy versions of Symantec AntiVirus:

■ If the System log becomes corrupted on a 64-bit client, you may see an
unspecified error message in the System logs on the Symantec Endpoint
Protection Manager console.
See "About recovering a corrupted client System Log on 64-bit computers"
on page 775.

■ When you use report and log filters, server groups are categorized as domains.
Client groups are categorized as groups, and parent servers are categorized
as servers.

■ If you generate a report that includes legacy computers, the IP address and
MAC address fields display **None**.

■ The reporting functions use a temporary folder, *drive*:\Symantec\Symantec
Endpoint Protection Manager\Inetpub\Reporting\Temp. You might want to

schedule your own automated tasks to periodically clean this temporary folder. If you do so, be sure that you do not delete the LegacyOptions.inc file, if it exists. If you delete this file, you lose the incoming data from legacy Symantec AntiVirus client logs.

Changing timeout parameters for reviewing reports and logs

If database errors occur when you view either reports or logs that contain a lot of data, you can make the following changes:

- Change the Microsoft SQL Server connection timeout

- Change the Microsoft SQL Server command timeout

The reporting defaults for these values are as follows:

- Connection timeout is 300 seconds (5 minutes)

- Command timeout is 300 seconds (5 minutes)

To change Microsoft SQL Server timeout values in Reporter.php

1   Browse to the following folder on the Symantec Endpoint Protection Manager server:

   drive:\Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\Reporting\Resources

2   Open the Reporter.php file with a plain-text editor, such as Notepad.

3   Find the **$CommandTimeout** line and increase the value (in seconds). If the line does not exist, create it. For example, to increase the timeout period to 10 minutes, change the line to the following value:

   $CommandTimeout = 600;

4   Find the **$ConnectionTimeout** line and increase the value (in seconds). If the line does not exist, create it. For example, to increase the timeout period to 10 minutes, change the line to the following value:

   $ConnectionTimeout = 600;

5   Save and close the Reporter.php file.

Note: If you specify zero, or leave the fields blank, the default setting is used.

If you get CGI or terminated process errors, you might want to change the following parameters:.

- max_execution_time parameter in the Php.ini file
- The Apache timeout parameters, FcgidIOTimeout, FcgidBusyTimeout, and FcgidIdleTimeout, in the httpd.conf file

To change timeout values in Php.ini

1 Browse to the *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\Php directory.

2 Right-click the Php.ini file, and then click **Properties**.

3 On the **General** tab, uncheck **Read-only**.

4 Click **OK**.

5 Open the Php.ini file with a plain-text editor, such as Notepad.

6 Locate the **max_execution_time** entry and increase the value (in seconds). For example, to increase the timeout to 10 minutes, change the line to the following value:

   max_execution_time=600

7 Save and close the Php.ini file.

8 Right-click the Php.ini file, and then click **Properties**.

9 On the **General** tab, check **Read-only**.

10 Click **OK**.

To change timeout values in httpd.conf

1 Browse to the *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\apache\conf directory.

2 Open the httpd.conf file with a plain-text editor, such as Notepad.

3 Locate the following lines and increase the values (in seconds):

   - FcgidIOTimeout 1800
   - FcgidBusyTimeout 1800
   - FcgidIdleTimeout 1800

4 Save and close the httpd.conf file.

Accessing reporting pages when the use of loopback addresses is disabled

If you have disabled the use of loopback addresses on the computer, the reporting pages do not display. If you try to log on to the Symantec Endpoint Protection

Manager console or to access the reporting functions, you see the following error message:

Unable to communicate with Reporting component

The **Home**, **Monitors**, and **Reports** pages are blank; the **Policies**, **Clients**, and **Admin** pages look and function normally.

To get the **Reports** components to display when you have disabled loopback addresses, you must associate the word localhost with your computer's IP address. You can edit the Windows hosts file to associate localhost with an IP address.

See "Logging on to reporting from a stand-alone Web browser" on page 614.

To associate localhost with the IP address on computers running Windows

1   Change directory to the location of your hosts file.

By default, the hosts file is located in *%SystemRoot%*\system32\drivers\etc

2   Open the hosts file with an editor.

3   Add the following line to the hosts file:

xxx.xxx.xxx.xxx **localhost** *#to log on to reporting functions*

where you replace *xxx.xxx.xxx.xxx* with your computer's IP address. You can add any comment you want after the pound sign (#). For example, you can type the following line:

192.168.1.100 localhost # this entry is for my console computer

4   Save and close the file.

About recovering a corrupted client System Log on 64-bit computers

If the **System** log becomes corrupted on a 64-bit client, you may see an unspecified error message in the **System** logs on the Symantec Endpoint Protection Manager console. If corrupted, you cannot view the data in the log on the client and the data does not upload to the console. This condition can affect data in the console **Computer Status**, **Risk**, and **Scan** logs and reports.

To correct this condition, you can delete the corrupted log file and the serialize.dat file on the client. These files are located on the client in Drive:\Documents and Settings\All Users\Application Data\Symantec\Symantec AntiVirus Corporate Edition\7.5\Logs*date*.Log. After you delete these files, the log file is recreated and begins to log entries correctly.

Section 7

Managing Symantec Network Access Control

778

Introducing Symantec Network Access Control

This chapter includes the following topics:

About Symantec Network Access Control

Symantec Network Access Control ensures that a company's client computers are compliant with the company's security policies before the computers are allowed to access the network.

When enforcement controls are not in place, your organization's data is vulnerable to intended loss or inadvertent loss. Recovering the data can result in down time and financial losses that are associated with lost productivity. To prevent these losses, Symantec Network Access Control controls on site and remote access to corporate network resources. Symantec Network Access Control provides a complete end-to-end network access control solution.

Symantec Network Access Control uses a Host Integrity policy and an optional Symantec Enforcer to discover and evaluate which computers are compliant. The clients that are not compliant are directed to a remediation server. The remediation server downloads the necessary software, patches, virus definition updates, and so on, to make the client computer compliant. Symantec Network Access Control also continually monitors endpoints for changes in their compliance status.

Symantec Network Access Control is a companion product to Symantec Endpoint Protection. Both products include Symantec Endpoint Protection Manager, which provides the infrastructure to install and manage the Symantec Network Access Control and Symantec Endpoint Protection clients.

See "About Symantec Endpoint Protection" on page 41.

See "About the types of enforcement in Symantec Network Access Control" on page 780.

See "How self enforcement works" on page 783.

About the types of enforcement in Symantec Network Access Control

Symantec Network Access Control provides different methods of enforcement to control access to your network.

Table 40-1 describes the differences between host-based enforcement and network-based enforcement.

Table 40-1   Types of enforcement

Type of enforcement	Description
Host-based self enforcement	Allows the client computers to obtain and run the software they need to automatically remediate compliance failures. When the client computer is remediated, it can safely access the network. Host-based enforcement uses the Symantec firewall to allow or block access. The firewall is included as part of the Symantec Endpoint Protection product.
	Host-based enforcement includes the following methods:
	■ Self-enforcement uses the firewall to police network access, providing the easiest and fastest enforcement deployment option. You can implement self-enforcement more easily if the organization has already deployed the Symantec Endpoint Protection product.
	■ Peer-to-peer enforcement ensures that client-to-client communication occurs only between the company computers and compliant computers outside the company. Compliant computers have the latest company security policy.
	See "About Host Integrity remediation" on page 824.
Network-based enforcement	Uses the Symantec Enforcer appliances and integrated software Enforcers to enable you to control network access. Network-based enforcement authenticates and allows network access only to the clients that meet the requirements in the Host Integrity policy. Network-based enforcement also checks that the policy is current.
	Additionally, if your deployment includes a Gateway Enforcer appliance, you can allow guests without compliant software to access your network temporarily. These Enforcers enable guest access by installing On-Demand clients on guest computers and dissolving them when guests log off. Guest access works with both Windows and Mac clients. This enforcement requires an Enforcer appliance.

How Symantec Network Access Control works

Symantec Network Access Control performs endpoint compliance by performing the following steps:

Table 40-2   Process that Symantec Network Access Control uses to check and remediate compliance on client computers

Step	Action	Description
1	Discovers all attempts to access your network.	The endpoint connects to the network. The Enforcer determines the endpoint's configuration.
2	Checks the compliance of the configuration against the policy.	Checks that all client computers that access your network meet your security policy requirements.
3	Takes action based on the outcome of policy check.	For the client computers that do not meet requirements, an Enforcer: ■ Remediates by downloading, installing, and running the software you require. ■ Allows limited access. ■ Allows complete access and log all network access attempts.
4	Monitors endpoint to ensure ongoing compliance.	Monitors and reports on Enforcers, system traffic, and compliance status.

Figure 40-1 shows how the Symantec Endpoint Protection Manager enforces the security policy on a managed client computer.

Figure 40-1   Symantec Network Access Control architecture
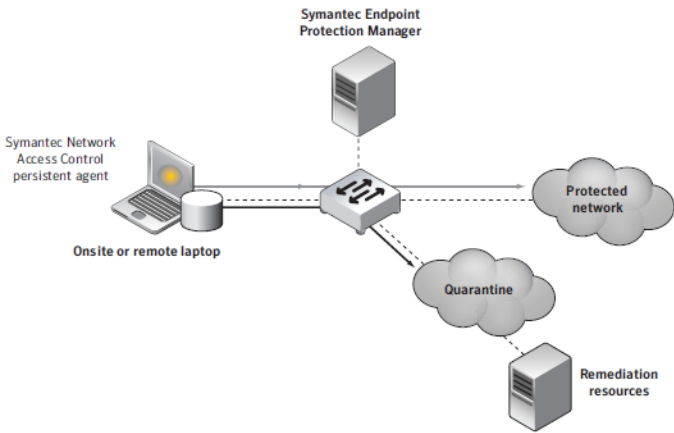
How self enforcement works

During the Host Integrity check, the client follows the requirements that are set in the Host Integrity policy. It examines active applications, date and size of a file, and other parameters. If these meet the Host Integrity policy's requirements, the client can access the network. If it does not, the client automatically generates a detailed message entry in the Security log for all failed requirements. The client then follows the remediation steps that you have designed in your Host Integrity policy. You may have set a policy that the client can access the network even if it fails the Host Integrity check. The likelier case is that you have set up remediation steps to bring the client into compliance with your security policies.

If the client computer cannot meet the requirements, the client can be set to silently connect to a remediation server. From there it can download and install the required software. The software can include a software patch, a hotfix, an update to virus definitions, and so on. The client can give the user a choice to download immediately or postpone a download. The policy can be set such that the computer cannot connect to the enterprise network until the software is installed.

See "What you can do with Host Integrity policies" on page 812.

Every time a client receives a new security policy, it immediately runs another Host Integrity check.

The client can be set up to automatically download and install the latest predefined or customized Host Integrity policies from the Symantec Endpoint Protection Manager. If the client cannot connect to the console, the Windows or Mac On-Demand client gets the Host Integrity policy from the Enforcer appliance when first downloaded. After that it gets the Host Integrity policy from the Symantec Endpoint Protection Manager.

You can consider some of the following examples when you set up the requirements for Host Integrity enforcement:

■ The client runs up-to-date antivirus software.

- The Host Integrity check is done only when the client tries to connect to the network through an Enforcer.
- The check triggers the actions that take place silently on the client.

You can also use an Enforcer to enforce these policies. The Enforcer is either a software application or an optional hardware appliance that mediates the connectivity of the client to the network. Most of the following examples show the use of an Enforcer.

The Enforcer can be configured to automatically do the following:

- Verify that a client has been installed on a user's computer.
- Prompt a client to retrieve updated security policies, if available.
- Prompt the client to run the Host Integrity check.

The client first verifies that the latest antivirus software is installed and runs it. If it has been installed but is not running, the client silently starts the antivirus application. If it is not installed, the client downloads the software from a URL that is specified in the Host Integrity requirement. Then the client installs and starts the software.

Next, the client verifies that the antivirus signature files are current. If the antivirus files are not current, the client silently retrieves and installs the updated antivirus files.

The client runs the Host Integrity check again and passes. The Enforcer receives the results and grants the client access to the enterprise network. In this example, the following requirements must be met:

- The file server that is used for Host Integrity updates has the latest files installed.
  The client obtains updated applications from the file server. You can set up one or more remediation servers that are connected to the enterprise network. From the remediation servers, users can copy or automatically download the required patches and hotfixes for any required application.
  If a remediation server fails, then Host Integrity remediation also fails. If the client tries to connect through an Enforcer, the Enforcer blocks the client if Host Integrity fails. If the client is connected to Symantec Endpoint Protection Manager, you can set the console to pass the Host Integrity check even though the check fails. In this case, the Enforcer can block the client. Information about the failed Host Integrity check is recorded in the client's Security log.
- The management server must be configured so that updates of the security policy are automatically sent to any computer that runs the client.

If the Enforcer blocks the client, the client tries to recover. The Host Integrity policy is set up to update files before it allows the client to connect to the network.

The user is then notified that an update needs to be provided. A progress indicator for the update follows the update.

See "Adding Host Integrity requirements" on page 817.

About the Symantec Network Access Control Enforcer appliances

Symantec Enforcer appliances are the optional network components that work with the Symantec Network Access Control clients.

Symantec Network Access Control comes with the following Linux-based Enforcer images, which you install on the Symantec Enforcer appliances:

- Symantec Network Access Control Gateway Enforcer appliance image
- Symantec Network Access Control LAN Enforcer appliance image

Additionally, all Windows-based Symantec Enforcers work with managed clients to protect your network. These clients include the Symantec Endpoint Protection client and the Symantec Network Access Control client.

See "Installing an Enforcer appliance" on page 800.

See "Installation planning for a Gateway Enforcer appliance" on page 857.

How the Symantec Network Access Control Enforcer appliances work with Host Integrity policies

The security policies that all Enforcer appliances direct Symantec Network Access Control or Symantec Endpoint Protection clients to run on client computers are called Host Integrity policies. You create and manage Host Integrity policies on the console of a Symantec Endpoint Protection Manager.

Host Integrity policies specify the software that is required to run on a client. For example, you can specify that the following security software that is located on a client computer must comply with certain requirements:

- Antivirus software
- Antispyware software
- Firewall software
- Patches
- Service packs

When a client tries to connect to the network, it runs a Host Integrity check. It then sends the results to an Enforcer appliance. You can configure clients to run Host Integrity checks at various times.

Typically, the Enforcer appliance is set up to verify that the client passes the Host Integrity check before it grants network access to the client. If the client passes the Host Integrity check, it is in compliance with the Host Integrity policy at your company. However, each type of Enforcer appliance defines the network access criteria differently.

See "How the Gateway Enforcer appliance works" on page 787.

See "How the LAN Enforcer appliance works" on page 788.

Communication between an Enforcer appliance and a Symantec Endpoint Protection Manager

The Enforcer appliance stays connected to the Symantec Endpoint Protection Manager. At regular intervals (the heartbeat), the Enforcer appliance retrieves settings from the management server. Those settings controls how the Enforcer appliance operates. When you make any changes on the management server that affect the Enforcer appliance, the Enforcer appliance receives the update during the next heartbeat. The Enforcer appliance transmits its status information to the management server. It can log the events that it forwards to the management server. The information then appears in the logs on the management server.

The Symantec Endpoint Protection Manager maintains a list of management servers with replicated database information. It downloads the management server list to connected Enforcers and managed clients and guest clients. If the Enforcer appliance loses communication with one management server, it can connect to another management server that is included in the management server list. If the Enforcer appliance is restarted, it uses the management server list to reestablish a connection to a management server.

When a client tries to connect to the network through the Enforcer appliance, the Enforcer appliance authenticates the client Globally Unique Identifier (GUID). The Enforcer appliance sends the GUID to the management server and receives an accept response or a reject response.

If an Enforcer appliance is configured to authenticate the GUID, it can retrieve information from the management server. The Enforcer appliance can then determine if the client profile has been updated with the latest security policies. If the client information changes on the management server, the management server can send the information to the Enforcer appliance. The Enforcer appliance can again perform host authentication on the client.

See "Changing Gateway Enforcer appliance configuration settings in Symantec Endpoint Protection Manager" on page 872.

See "Changing LAN Enforcer configuration settings in Symantec Endpoint Protection Manager" on page 920.

Communication between the Enforcer appliance and clients

The communication between the Enforcer appliance and a client begins when the client tries to connect to the network. The Enforcer appliance can detect whether a client is running. If a client is running, the Enforcer begins the authentication process with the client. The client responds by running a Host Integrity check and by sending the results, along with its profile information, to the Enforcer.

The client also sends its Globally Unique Identifier (GUID), which the Enforcer passes on to the management server for authentication. The Enforcer appliance uses the profile information to verify that the client is up to date with the latest security policies. If not, the Enforcer appliance notifies the client to update its profile.

After the Gateway Enforcer appliance allows the client to connect, it continues to communicate with the client at regular predefined intervals. This communication enables the Enforcer appliance to continue to authenticate the client. For the LAN Enforcer appliance, the 802.1x switch handles this periodic authentication. For example, the 802.1 switch starts a new authentication session when re-authentication time comes.

The Enforcer appliance needs to run at all times; otherwise the clients that try to connect to the corporate network may be blocked.

See "Creating and testing a Host Integrity policy" on page 812.

How the Gateway Enforcer appliance works

Gateway Enforcer appliances perform one-way checking. They check the clients that try to connect through the Gateway Enforcer appliance's external NIC to the organization's network.

A Gateway Enforcer appliance uses the following processes to check client computers and determine if they can access the network:

■ The Gateway Enforcer appliance checks for client information and verifies that the client has passed the Host Integrity check.
See "How the Symantec Network Access Control Enforcer appliances work with Host Integrity policies" on page 785.

■ If the client satisfies the requirements for access, the Gateway Enforcer appliance connects it to the network.

■ If a client does not satisfy the requirements for access, you can set up the Gateway Enforcer appliance to perform the following actions:

■ Monitor and log certain events.

■ Block users if the Host Integrity check failed.

■ Display a pop-up message on the client.

■ Provide the client with limited access to the network to allow the use of network resources for remediation.
To provide limited access, you redirect client HTTP requests to a Web server with remediation information. For example, this Web server can include instructions on where to obtain remediation software. Or, it can allow the client to download the Symantec Network Access Control client software.

■ Allow the client to access the network even though it has failed the Host Integrity check.
The Gateway Enforcer appliance has the following optional configuration capabilities:

■ Allow the client computers with trusted IP addresses to access the network immediately.
You can configure which client IP addresses to check and which IP addresses are trusted. Clients with trusted IP addresses are granted access without additional authentication.

■ Allow the computers that do not run Windows to access the network.
In this case, the Gateway Enforcer appliance functions as a bridge instead of a router. As soon as a client is authenticated, the Gateway Enforcer appliance forwards packets to allow the client to have access to the network.
See About the LAN Enforcer appliance installation on page 785.
See "What you can do with Symantec Enforcer appliances" on page 793.
See "About installing an Enforcer appliance" on page 800.

How the LAN Enforcer appliance works

The LAN Enforcer appliance gives you the option of 802.1x EAP (Extensible Authentication Protocol) authentication along with the having the client perform a Host Integrity check.

Note: For details on EAP, refer to the IETF's RFC 2284 at PPP Extensible Authentication Protocol (EAP). For additional details on IEEE Standard 802.1x, refer to the text of the standard at IEEE8021-PAE-MIB Definitions.

You can deploy the LAN Enforcer using one of the following modes:

■ Transparent mode: Checks if the client is compliant with Host Integrity security policy but does not check the user name and password. Transparent mode does not use a RADIUS server, but requires an 802.1x-capable switch.

■ Full 802.1x mode: Authenticates the user's credentials (user name and password) in addition to having the client check for host authentication. Non-compliant clients are routed to a guest VLAN that your organization has set up for client security remediation. Full 802.1x authentication requires a RADIUS server, an 802.1x-capable switch or wireless access point, and supplicant (client) software.

In transparent mode, a LAN Enforcer appliance uses the following methods to process client computer requests to access the network:

■ The client computer connects and sends logon, host authentication compliance, and policy data through EAP.

■ The switch or wireless access point forwards the client computer data to the LAN Enforcer appliance.

■ The LAN Enforcer appliance verifies that the client has passed a Host Integrity check.
See "How the Symantec Network Access Control Enforcer appliances work with Host Integrity policies" on page 785.

■ If the client passes the Host Integrity check, the Enforcer opens a part of the switch and allows full network access.

■ If the client fails the Host Integrity check, the Enforcer assigns the client to a quarantine VLAN where it can access remediation resources.

In full 802.1x mode, a LAN Enforcer appliance does the following to process client computer requests to access the network:

■ The client computer connects and sends logon, host authentication compliance, and policy data through EAP.

■ The supplicant on the client computer asks the user for their user name and password.

■ The switch forwards the user name and password to the LAN Enforcer.

■ The LAN Enforcer forwards the user name and password to the RADIUS server.

■ The RADIUS server generates an EAP challenge (user name and password).

- The LAN Enforcer receives the EAP challenge and adds the Host Integrity check.

- The LAN Enforcer verifies that the client has passed the Host Integrity check.

- The LAN Enforcer checks the Host Integrity results and forwards them to the RADIUS server.

- The RADIUS server performs EAP authentication and sends the result to the LAN Enforcer.

- The LAN Enforcer receives the authentication result and forwards it and the action to take to the switch.

- If the client passes the EAP and Host Integrity challenges, the switch allows network access.

- If the client does not pass the challenges, the switch routes it to an alternate VLAN where it can access remediation resources.

The LAN Enforcer appliance has the following additional optional configuration capabilities. You can:

- Use a switch or wireless access point to direct the client to a remediation VLAN. (Recommended)

- Configure the possible failure responses, depending on whether you use EAP authentication or Host Integrity checking.

- Connect multiple LAN Enforcer appliances to one switch for LAN Enforcer failover.

- Configure multiple RADIUS servers for RADIUS server failover.

How an Integrated Enforcer for Microsoft DHCP Servers works

The Integrated Enforcer for Microsoft DHCP Servers checks for Symantec Endpoint Protection or Symantec Network Access Control client installations on the DHCP clients that the DHCP server manages. It then enforces policies for those clients, as configured on the Symantec Endpoint Protection Manager.

The Integrated Enforcer for Microsoft DHCP Servers also authenticates the client for:

- The existence of an agent.

- A Globally Unique Identifier (GUID).

■ Host Integrity compliance.

■ The profile version of each configured policy.

The Integrated Enforcer for Microsoft DHCP Servers is a software component that interacts with the Microsoft DHCP Server. Although both must be installed on the same computer, the Integrated Enforcer for Microsoft DHCP Servers is not dependent on the DHCP server. When the Integrated Enforcer for Microsoft DHCP Servers resides on the same computer as the DHCP Server, it eliminates the need for additional hardware.

Note: Stopping the DHCP server does not stop the Integrated Enforcer for Microsoft DHCP Servers. Stopping the Integrated Enforcer for Microsoft DHCP Servers does not stop the DHCP server.

You use the Symantec Endpoint Protection Manager to configure the security policies. However, the Integrated Enforcer for Microsoft DHCP Servers enforces the security policies.

The Integrated Enforcer for Microsoft DHCP Servers authenticates the client computers by checking for the response for the following criteria:

■ Does the Symantec Endpoint Protection client or the Symantec Network Access Control client run on a client computer?

■ Does the Symantec Endpoint Protection client or the Symantec Network Access Control client have the correct Globally Unique Identifier (GUID)?
 Is the GUID a 128-bit hexadecimal number? This number is assigned to a client computer that runs the Symantec Endpoint Protection client or the Symantec Network Access Control client. The management server generates a GUID when the client initially connects.

■ Does the client comply with the latest Host Integrity policy that the administrator has set up on the console of the Symantec Endpoint Protection Manager?

■ Has the client received the latest security policy?

If the Integrated Enforcer for Microsoft DHCP Servers cannot authenticate the client, it provides access to a quarantined area. The quarantine area provides limited network resources to the client. The quarantine area is configured on the same computer as the Integrated Enforcer for Microsoft DHCP Servers and the Microsoft DHCP server.

You can also set up access to a remediation server. The remediation server provides clients with links to software that enables them to become compliant with your security policies.

See "About the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers" on page 983.

How an Integrated Enforcer for Microsoft Network Access Protection works with a Microsoft Network Policy Server (NPS)

The Integrated Enforcer for Microsoft Network Access Protection works by allowing you to extend the capabilities of Microsoft Network Access Protection (NAP), including:

■ Checking for adherence to endpoint security policies. Connecting clients can use the same polices or different policies.

■ Controlling guest access.

■ Authenticating end users.

When you configure a Network Policy Server (NPS) as a NAP policy server, it evaluates statements of health (SoH) sent by NAP-capable clients. If the clients are healthy, they can connect to the network.

You can configure NAP policies on NPS that allow client computers to update their configuration to become compliant with your organization's security policy. You configure those policies by following the instructions in the NPS documentation.

See "About the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection" on page 984.

How the On-Demand Client works

The On-Demand Client checks your computer for compliance if you try to connect your computer to a protected network as a guest. If the client computer meets all requirements, a connection between the client computer and the Symantec Endpoint Protection Manager is automatically established. If the client meets all security requirements, the client can then access the protected network.

At that point, the security-compliant client computer can perform any task that the administrator has enabled for this group on the Symantec Endpoint Protection Manager. If the client computer cannot meet all security requirements, a connection between the client computer and the protected network cannot be automatically established. The user needs to remediate all noncompliant requirements on the client computer by downloading the remediation files as set

up by the administrator. Until the remediation is complete, the client cannot access the protected network as a guest.

Your computer must pass or fail a Compliance Status Check when it tries to connect to a company's protected network. Therefore the access status to a company's protected network is as follows:

- Allowed—You can connect to the network. In Allowed mode there is no communication with an Enforcer, or an Enforcer is not installed in the network.

- Approved—You are approved to connect to the network by Symantec Network Access Control.

- Quarantined—The Symantec Network Access Control has placed you in a quarantine area because your compliance status has failed or the policy is not the latest one.

See "Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network" on page 1054.

What you can do with Symantec Enforcer appliances

The Enforcer appliance is installed at network endpoints for external clients or internal clients.

For example, you can install an Enforcer appliance between the network and a VPN server. You can also set up enforcement on the client computers that connect to the network with an 802.1x-aware switch or a wireless access point.

An Enforcer appliance performs host authentication rather than user-level authentication. It ensures that the client computers that try to connect to an enterprise network comply with the security policy of that enterprise. You can configure specific security policies on the Symantec Endpoint Protection Manager.

If the client does not comply with the security policies, the Enforcer appliance can take the following actions:

- Block access to the network.

- Allow access to limited resources only.

- Allow access when the client is non-compliant, and log that action.

The Enforcer appliance can redirect the client to a quarantine area with a remediation server. The client can then obtain the required software, applications, signature files, or patches from the remediation server.

For example, part of a network may already be configured for the clients that connect to the local area network (LAN) through 802.1x-aware switches. If that is the case, you can use a LAN Enforcer appliance for these clients.

You can also use a LAN Enforcer appliance for the clients that connect through a wireless access point that is 802.1x-enabled.

See "How the LAN Enforcer appliance works" on page 788.

See "Planning for the installation of a LAN Enforcer appliance" on page 909.

If you have employees who work remotely and connect through a VPN, you can use the Gateway Enforcer appliance for those clients.

You can also use the Gateway Enforcer appliance if a wireless access point is not 802.1x-enabled.

See "How the Gateway Enforcer appliance works" on page 787.

See "Installation planning for a Gateway Enforcer appliance" on page 857.

If high availability is required, you can install two or more Gateway or LAN Enforcer appliances at the same location to provide failover.

See "Failover planning for Gateway Enforcer appliances" on page 866.

See "Failover planning for LAN Enforcer appliances and RADIUS servers" on page 913.

If you want to implement high availability for LAN Enforcer appliances, you must install multiple LAN Enforcer appliances and an 802.1x-aware switch. High availability is accomplished through the addition of an 802.1x-aware switch. If you only install multiple LAN Enforcer appliances without an 802.1x-aware switch, then high availability fails. You can configure an 802.1x-aware switch for high availability.

For information about the configuration of an 802.1x-aware switch for high availability, see the accompanying documentation for the 802.1x-aware switch.

In some network configurations, a client may connect to a network through more than one Enforcer appliance. After the first Enforcer appliance provides authentication to the client, the remaining Enforcer appliances authenticate the client before the client can connect to the network.

What you can do with Symantec Integrated Enforcers

The optional Symantec Network Access Control Integrated Enforcers are Enforcers provided as software components. You can configure them to ensure that the clients that try to connect to the network comply with your organization's configured security policies.

■ Use the Symantec Network Access Control Integrated Enforcer for DHCP Servers to ensure that a Microsoft DHCP Server's clients comply with security policies.

■ Use the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection to ensure that clients comply with Microsoft client health policies. You can also use the Symantec Health Agent to check Symantec health policies in addition to Microsoft health policies.

You can perform the following key tasks with the Integrated Enforcers:

■ Ensure that client computers that attempt to connect to the network comply with the security policies you set on the Symantec Endpoint Protection Manager.

■ Configure a connection to a Symantec Endpoint Protection Manager.

■ Start and stop the Enforcer service.

■ View the connection status.

■ View Security and System logs on the Symantec Endpoint Protection Manager.

See "How an Integrated Enforcer for Microsoft DHCP Servers works" on page 790.

See "How an Integrated Enforcer for Microsoft Network Access Protection works with a Microsoft Network Policy Server (NPS)" on page 792.

What you can do with On-Demand Clients

When users cannot connect to your network because they lack the required compliance software, you can provide them with On-Demand clients. When an On-Demand client is installed, it authenticates the user and ensures that the computer passes a compliance check before it accesses the network. On-Demand clients stay in effect until the guest logs off. They are available for both Windows and Macintosh guest computers.

On-Demand clients protect your network's sensitive business information from data loss. With an On-Demand client, guests and remote staff can connect to your network through Web-enabled applications without introducing spyware, keyloggers, and other malware that can infect your network.

The provisioning process requires:

■ A Gateway Enforcer configured to provide On-Demand clients.

■ An On-Demand client download and installation on guest computers

See "Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network" on page 1054.

See "Setting up authentication on the Gateway Enforcer console for Symantec Network Access Control On-Demand clients" on page 1056.

Installing Symantec Network Access Control

This chapter includes the following topics:

- Deploying Symantec Network Access Control
- Upgrading Symantec Endpoint Protection Manager to include Symantec Network Access Control
- About installing an Enforcer appliance
- Installing an Enforcer appliance
- About the Enforcer appliance indicators and controls
- Setting up an Enforcer appliance
- Logging on to an Enforcer appliance
- Configuring an Enforcer appliance

Deploying Symantec Network Access Control

It is best to deploy Symantec Network Access Control in phases. This approach allows your organization to evolve an implementation that fits your needs. You build on each previous phase instead of completely redoing your entire security infrastructure to make changes or enhancements.

Table 41-1   Phases for deploying Symantec Network Access Control

Phase	Action	Description
Phase 1	Install Symantec Endpoint Protection Manager and Symantec Network Access Control clients. Use Symantec Endpoint Protection Manager to configure Host Integrity policies.	You can control access for the laptops, desktops, and servers your organization that manages with self-enforcement. With self-enforcement, computers can obtain the software they need to comply with your security policy.
		See "Getting up and running on Symantec Endpoint Protection for the first time" on page 51.
		See "How self enforcement works" on page 783.
		See "Creating and testing a Host Integrity policy" on page 812.
		See "Upgrading Symantec Endpoint Protection Manager to include Symantec Network Access Control" on page 799.
Phase 2	Install and configure a Gateway Enforcer appliance.	For partial network protection, control wired and wireless access to the network for managed and unmanaged clients and for guest computers.
		Managed clients are those that running the Symantec Network Access Control client.
		Unmanaged clients are those that:
		■ Are not running Symantec Network Access Control client software. ■ Are running Symantec Network Access Control client software, but do not have the latest policy updates.
		Guest clients are the laptops, desktops, and servers that do not meet your security requirements for items such as installed software and secure passwords. These are devices owned by guests such as contractors, consultants, and partners. You can allow these guest clients to safely and temporarily connect to your network with On-Demand clients.
		See "About installing an Enforcer appliance" on page 800.
		See "Installing an Enforcer appliance" on page 800.
		See "How the Gateway Enforcer appliance works" on page 787.
		See "How the On-Demand Client works" on page 792.

Table 41-1   Phases for deploying Symantec Network Access Control *(continued)*

Phase	Action	Description
Phase 3	Install and configure a LAN Enforcer appliance	For complete network protection, you can control LAN access for client computers and guest computers. ■ For managed clients, use a LAN Enforcer appliance. ■ For unmanaged clients, use the LAN or Gateway Enforcer appliances. See "About installing an Enforcer appliance" on page 800. See "Installing an Enforcer appliance" on page 800. See "How the LAN Enforcer appliance works" on page 788.

See "About the types of enforcement in Symantec Network Access Control" on page 780.

Upgrading Symantec Endpoint Protection Manager to include Symantec Network Access Control

If you already have installed Symantec Endpoint Protection, you can upgrade Symantec Endpoint Protection to include Symantec Network Access Control. Symantec Network Access Control includes two separate components: the Symantec Endpoint Protection Manager and the Symantec Network Access Control client.

If you have already installed Symantec Endpoint Protection Manager for Symantec Endpoint Protection, you can now upgrade your Symantec Endpoint Protection Manager installation and install the Symantec Network Access Control client.

To upgrade Symantec Endpoint Protection Manager to include Symantec Network Access Control

1   Insert the product disc for Symantec Network Access Control.

   If the installation program does not start immediately, open the disc and double-click `setup.exe`.

2   In the **Symantec Endpoint Protection Installation** dialog box, click **Install Symantec Network Access Control**.

3   In the next **Symantec Endpoint Protection Installation** dialog box, click **Install Symantec Endpoint Protection Manager**.

4   In the **Welcome to the Management Server Upgrade Wizard** dialog box, click **Next**.

5 After the wizard completes, in the **Management Server and Console Installation Summary** dialog box, click **Next**, and then click **Finish**.

6 After the upgrade, the **Welcome to the Management Server Configuration Wizard** dialog box appears. Provide the appropriate values, click **Next**, and then click **Finish**.

7 Deploy the Symantec Network Access Control client.

See "About client deployment methods" on page 131.

About installing an Enforcer appliance

You select the type of Enforcer appliance that you want to use during the installation process. Before you start to install any of the Enforcer appliances:

- Familiarize yourself with the locations of the components in your network.

- Locate the Symantec Network Access Control Enforcer installation Disc 2. This disc contains the software for all the types of Symantec Network Access Control Enforcer appliances.

- Identify the host name that you want to assign to the Enforcer appliance. The default host name is Enforcer. You may want to change this name to make it easier to identify each Enforcer appliance in a network.

- Identify the IP addresses of the network interface cards (NICs) on the Enforcer appliance.

- Identify the IP address, host name, or domain ID of the Domain Name Server (DNS), if applicable. Only DNS servers can resolve host names.
  If you want the Enforcer appliance to connect to a Symantec Endpoint Protection Manager by using a host name, it needs to connect to a DNS server. You can configure the IP address of the DNS server during the installation. However, you can use the configure DNS command to change the IP address of a DNS server from the Enforcer console with the Configure DNS command.

See "Installing an Enforcer appliance" on page 800.

Installing an Enforcer appliance

Table 41-2 lists the steps to install all types of Enforcer appliances.

| | Table 41-2 | Installation summary for an Enforcer appliance |

Step	Action	Description
Step 1	Learn where to place Enforcers in your network.	Enforcers need to be placed in specific locations on your network to ensure that all endpoints comply with your security policy. See "Installation planning for a Gateway Enforcer appliance" on page 857. See "Where to place LAN Enforcer appliances" on page 910.
Step 2	Set up the appliance.	Connect the Enforcer appliance to your network. See "About installing an Enforcer appliance" on page 800. See "About the Enforcer appliance indicators and controls" on page 801. See "Setting up an Enforcer appliance" on page 803.
Step 3	Configure the appliance.	Log on and configure the Enforcer appliance from the Enforcer command line. See "Logging on to an Enforcer appliance" on page 804. See "Configuring an Enforcer appliance" on page 805.

About the Enforcer appliance indicators and controls

The Enforcer appliance is installed on a 1U rack-mountable chassis with support for static rails.

Figure 41-1 shows the controls, indicators, and connectors that are located behind the optional bezel on the front panel.

Figure 41-1 Enforcer appliance front panel
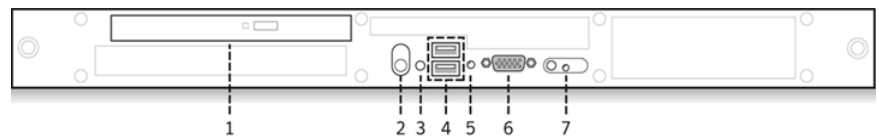
1	DVD-ROM drive
2	Power switch
3	Reset icon
4	USB ports
5	Hard drive light

| 6 | Monitor |
| 7 | Reserved; do not use |

Figure 41-2 shows the back panel of the system.

Figure 41-2   Enforcer appliance back panel (Failopen model shown)
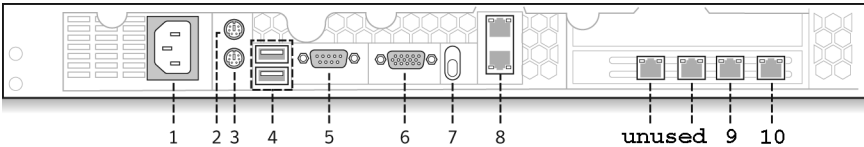
1	Power cord connector
2	Mouse connector
3	Keyboard connector
4	USB ports
5	Serial port
6	Monitor
7	Reserved; do not use
8	Reserved network ports; do not use
9	eth0 network port
10	eth1 network port

You can use the provided serial port and the serial cable to connect to another system that is hooked up to a monitor and keyboard. Alternatively, you can connect a monitor or keyboard directly. If you connect by using the serial port, the default baud rate that is set on the Enforcer is 9600 bps. You must configure the connection on the other system to match. Connecting by the serial port is the preferred method. It lets you transfer files, such as debugging information, to the connected computer for troubleshooting.

See "Installing an Enforcer appliance" on page 800.

See "Setting up an Enforcer appliance" on page 803.

Setting up an Enforcer appliance

Set up the Enforcer appliance hardware by connecting it to your network, switching it on, and logging on at the command line.

See

See

To set up an Enforcer appliance

1   Unpack the Enforcer appliance.

2   Mount the Enforcer appliance in a rack or place it on a level surface.

    See the rack mounting instructions that are included with the Enforcer appliance.

3   Plug it into an electrical outlet.

4   Connect the Enforcer appliance by using one of the following methods:

    ■ Connect another computer to the Enforcer appliance by using a serial port.
      Use a null modem cable with a DB9 connector (female). You must use terminal software, such as HyperTerminal, CRT, or NetTerm, to access the Enforcer console. Set your terminal software to 9600 bps, data bits 8, no parity, 1 stop bit, no flow control.

    ■ Connect a keyboard and VGA monitor directly to the Enforcer appliance.

5   Connect the Ethernet cables to the network interface ports as follows:

Gateway Enforcer appliance	Connect two Ethernet cables. One cable connects to the eth0 port (internal NIC). The other cable connects to the eth1 port (external NIC) on the rear of the Enforcer appliance.
	The internal NIC connects to the protected network and the Symantec Endpoint Protection Manager. The external NIC connects to the endpoints.
LAN Enforcer appliance	Connect one Ethernet cable to the eth0 port on the rear of the Enforcer appliance. This cable connects to the internal network. The internal network connects to an 802.1x-enabled switch and to any additional 802.1x-enabled switches in your network.

6   Switch on the power.

    The Enforcer appliance starts.

Logging on to an Enforcer appliance

When you turn on or restart the Enforcer appliance, the logon prompt for the Enforcer appliance console appears:

```
Enforcer Login
```

The following levels of access are available:

Superuser	Access to all commands
Normal	Access only to the `clear`, `exit`, `help`, and `show` commands for each level of the command hierarchy

Note: The Enforcer appliance automatically logs users off after 90 seconds of inactivity.

See "Setting up an Enforcer appliance" on page 803.

To log on to an Enforcer appliance with access to all commands

1   On the command line, log on to an Enforcer appliance with access to all commands by typing the following command:

    ```
    root
    ```

2   Type the password that you created during the initial installation.

    The default password is `symantec`.

    The console command prompt for root is `Enforcer#`.

To log on to an Enforcer appliance with limited access to commands

1   If you want to log on to an Enforcer appliance with limited access to commands, type the following command on the command line:

    ```
    admin
    ```

2   Type the password on the command line.

    The default password is `symantec`.

    The console command prompt for admin is `Enforcer$`.

See "Configuring an Enforcer appliance" on page 805.

Configuring an Enforcer appliance

After you log on to the Enforcer appliance, you can configure the appliance from the Enforcer command-line interface.

To configure an Enforcer appliance

1   Specify the type of Enforcer appliance as follows, responding to the prompts from the Enforcer:

    ```
    1. Select Enforcer mode
    [G] Gateway  [L] LAN
    ```

    Where:

    G   Gateway Enforcer appliance

    L   LAN Enforcer appliance

2   Change the host name of the Enforcer appliance, or press **Enter** to leave the host name of the Enforcer appliance unchanged.

    The default host name of the Enforcer appliance is Enforcer. The name of the Enforcer appliance automatically registers on the Symantec Endpoint Protection Manager during the next heartbeat.

    At the prompt, type the following command if you want to change the host name of the Enforcer appliance:

    ```
    2. Set the host name
    Note:
    1) Input new hostname or press "Enter" for no change. [Enforcer]:
    ```

    hostname *hostname*

    where *hostname* is the new host name for the Enforcer appliance.

    Be sure to register the host name of the Enforcer appliance on the Domain Name Server itself.

3   Type the following command to confirm the new host name of the Enforcer appliance:

    ```
    show hostname
    ```

4   Type the IP address of the DNS server and press **Enter**.

5 Type the new root password at the prompt by first typing the following command:

```
password
```

```
Old password: new password
```

You must change the root password that you used to log on to the Enforcer appliance. Remote access is not enabled until you change the password. The new password must be at least nine characters long, and contain one lowercase letter, one uppercase letter, one digit, and one symbol.

6 Type the new admin password.

7 Set the time zone by following these prompts.

```
Set the time zone
Current time zone is [+0000]. Change it? [Y/n]
If you click 'Y', follow the steps below:
1) Select a continent or ocean
2) Select a country
3) Select one of the time zone regions
4) Set the date and time
Enable the NTP feature [Y/n]
Set the NTP server:
Note: We set up the NTP server as an IP address
```

8 Set the date and time.

9 Configure the network settings and complete the installation, following the Enforcer prompts.

```
Enter network settings

Configure eth0:
Note: Input new settings.
IP address []:
Subnet mask []:
Set Gateway? [Y/n]
   Gateway IP[]:

   Apply all settings [Y/N]:
```

See "Logging on to an Enforcer appliance" on page 804.

See "About the Enforcer appliance CLI command hierarchy" on page 855.

Chapter **42**

Upgrading and reimaging all types of Enforcer appliance images

This chapter includes the following topics:

- About upgrading and reimaging Enforcer appliance images
- Enforcer hardware compatibility matrix
- Determining the current version of an Enforcer appliance image
- Upgrading the Enforcer appliance image
- Reimaging an Enforcer appliance image

About upgrading and reimaging Enforcer appliance images

Determine the version of your Enforcer appliance software before you plan to upgrade or reimage any of the Enforcer appliance software.

See "Determining the current version of an Enforcer appliance image" on page 808.

You may need to upgrade the image of an Enforcer appliance to the current version if you want to connect to the most current version of Symantec Endpoint Protection Manager. The upgrade enables you to take advantage of the new features that the Symantec Network Access Control Enforcer appliance provides. The Enforcer appliances works with Symantec Endpoint Protection Manager 11.0 and all subsequent versions and release updates.

You can select any of the following methods to upgrade the Enforcer appliance image:

■ Upgrade the current Enforcer appliance image.
See "Upgrading the Enforcer appliance image" on page 809.

■ Install a different Enforcer appliance image over a previous Enforcer appliance image.
See "Reimaging an Enforcer appliance image" on page 809.

Enforcer hardware compatibility matrix

Enforcer hardware compatibility matrix lists Symantec Network Access Control appliance image releases and their level of testing and support for Dell Enforcer appliance hardware models.

Table 42-1   Enforcer hardware compatibility matrix

Image version	Dell PE 850	Dell PE 860	Dell R200	Dell R210
Image version 12.1	Not supported	Partially tested and fully supported	Fully tested and fully supported	Fully tested and fully supported
Image version 11.0.6100 and above (RU6 MP1 and above)	Partially tested and fully supported	Partially tested and fully supported	Fully tested and fully supported	Fully tested and fully supported
Image version 11.0.6	Fully tested and fully supported	Fully tested and fully supported	Fully tested and fully supported	Not supported
Image versions 11.0.2, 11.0.3, 11.0.4, and 11.0.5	Fully tested and fully supported	Fully tested and fully supported	Fully tested and fully supported	Not supported
Image version 11.0.0, 11.0.1	Fully tested and fully supported	Fully tested and fully supported	Not supported	Not supported

Determining the current version of an Enforcer appliance image

You should determine the current version of the image that is supported on the Enforcer appliance. You should try to upgrade if you do not have the latest version.

To check the current version of an Enforcer appliance image, type the following command on the command-line interface of an Enforcer appliance: **show version**

Upgrading the Enforcer appliance image

You can use any of the following methods to update an Enforcer appliance image to the latest image:

- Upgrade the Enforcer appliance image from 5.1.x to the current version with a USB (Universal Serial Bus) disk.
- Upgrade the Enforcer appliance image from 5.1.x to the current version from a TFTP server.

To upgrade the Enforcer appliance image from 5.1.x with a USB disk

1   Copy the two update files, `initrd-Enforcer.img.gpg` and `package list`, to a USB disk.

2   Type the following command to automatically update the Enforcer appliance:

    Enforcer# `update`

To upgrade the Enforcer appliance image from 5.1.x with a TFTP server

1   Upload the two update files, `initrd-Enforcer.img.gpg` and `package list` to a Trivial File Transfer Protocol (TFTP) server to which an Enforcer appliance can connect.

2   Run the following command on the console of the Enforcer appliance:

    Enforcer:# `update tftp://`*IP address of TFTP server*

3   Select **Y** when you are prompted to launch the new image.

4   Select **1** to restart the Enforcer appliance after you apply a new image.

    Do not launch the new image without restarting the Enforcer appliance.

5   Log on to the Enforcer appliance.

6   See "Logging on to an Enforcer appliance" on page 804.

Reimaging an Enforcer appliance image

The Enforcer appliance comes with reimaging software for all Enforcer appliances: Gateway and LAN. The reimaging software includes the hardened Linux operating system and the Enforcer appliance software for replacement of an Enforcer appliance image.

When you start the installation from disc 2, the reimaging process erases the existing configuration on the Enforcer appliance. New files are installed over all existing files. Any configuration that was previously set on the Enforcer appliance is lost.

You can install a different type of Enforcer appliance image if you want to change the type that you use. If you change the type of Enforcer appliance image, it may involve the relocation of an Enforcer appliance in the corporate network.

When you reimage an Enforcer, you should also discard all group information related to that Enforcer that was stored in Symantec Endpoint Protection Manager. You are starting from the beginning with the new type of Enforcer. The Enforcer discards all previous Symantec Endpoint Protection Manager group information completely. You must create a new share key, and Symantec Endpoint Protection Manager group information should be re-configured manually as needed to ensure proper coordination.

To reimage an Enforcer appliance

1   Insert product disc 2 in the disc drive of the Enforcer appliance.

2   On the command line, type the following command:

Enforcer:# `reboot`

This command restarts the Enforcer appliance.

3   In the **Setup** menu, select **Setup Symantec Enforcer** from the product disc.

If you do not use the **Setup** menu, the Enforcer appliance restarts from the hard disc instead of the product disc. To reimage, you must restart from the disc.

4   Install and configure the Enforcer appliance.

See "About installing an Enforcer appliance" on page 800.

Customizing Host Integrity policies

This chapter includes the following topics:

What you can do with Host Integrity policies

Use Host Integrity policies to make sure that the client computers that access your network meet your organization's security policy. For example, you can use Host Integrity policies to ensure that client computers:

■ Are running virus protection and spyware protection applications. If they do not, allow them to remediate by downloading and installing the required virus and spyware protection applications.

■ Have passed virus protection checks done by Symantec Endpoint Protection on Windows platforms. If Symantec Endpoint Protection is not installed, this check will report as a host integrity failure, and will appear in the Security log.

■ Have the latest virus definitions. If they do not, automatically download virus definition updates.

■ Have the latest patches and service packs. If they do not, allow them to remediate by downloading and installing the required patch or service pack.

■ Use strong passwords and change them as frequently as required.

■ Be more secure in general. For example, disabling remote desktop access if needed, controlling the adding and removing of programs, controlling the use of registry tools, and so on.

■ Have backup software installed. If they do not, allow them to remediate by downloading and installing the required backup software.

■ Have the software that lets you perform remote installations. If they do not, allow them to remediate by downloading and installing the required remote installation software, possibly using a custom script created by the administrator.

See "Creating and testing a Host Integrity policy" on page 812.

Creating and testing a Host Integrity policy

The Host Integrity policy is the foundation of Symantec Network Access Control. The policy that you create for this test is for demonstration purposes only. The policy detects the existence of an operating system and, when detected, generates a fail event. Normally, you would generate fail events for other reasons.

Note: If you purchased and installed Symantec Network Access Control and Symantec Endpoint Protection, you can create a Firewall policy for the client computers that fail Host Integrity. If you run Symantec Enforcer with Symantec Network Access Control, you can isolate the clients that fail Host Integrity to specific network segments. This isolation prevents client authentication and domain access.

Take the following steps to test a Host Integrity policy:

- Download the latest Host Integrity content from Symantec.

- Create a Host Integrity policy to test.

- Test the Host Integrity policy you have created.

To download the latest Host Integrity content from Symantec

1   In the management console, click **Admin** > **Servers**, and then click **Local Site**.

2   Under **Tasks**, click **Edit Site Properties**.

3   In the **Site Properties for Local Site** dialog box, on the **LiveUpdate** tab, click **Edit Source Servers**.

4   In the **Live Update Servers** dialog, check that the management server uses the correct LiveUpdate server, and then click **OK**.

    You can use the default Symantec LiveUpdate server, or use a specified internal LiveUpdate server. If you use an internal LiveUpdate server ensure that the Host Integrity content for the Windows or Mac operating systems is present and available.

5   Under **Content Types to Download**, click **Change Selection**.

6   In the **Content Types to Download** dialog box, make sure **Host Integrity content** is checked, and then click **OK**.

7   Click **OK**.

8   Under **Tasks**, click **Download LiveUpdate content**, and then click **Download**.

9   In the **Show LiveUpdate Status** dialog box, after any new content downloads to the management server, click **Close**.

    You can now access the templates in the Host Integrity policy.

To create a Host Integrity policy

1   In the console, click **Policies** > **Host Integrity**.

2   Under **Tasks**, click **Add a Host Integrity policy**.

3   In the **Policy Name** tab, type a policy name, and then click **Requirements**.

4   In the **Requirements** pane, make sure that **Always do Host Integrity checking** is checked, and then click **Add**.

5   In the **Add Requirement** dialog box, under **Select requirement**, click **Custom requirement**, and then click **OK**.

6   in the **Name** box, type a name for the Custom Requirement.

7   In the **Custom Requirement** dialog box, under **Customized Requirement Script**, right-click **Insert statements below**, and then click **Add > IF .. THEN**.

8   In the right pane, in the **Select a condition** drop-down menu, click **Utility: Operating System is**.

9   Under **Operating system**, check one or more operating systems that your client computers run and that you can test.

10   Under **Customized Requirement Script**, right-click **THEN //Insert statements here**, and then click **Add > Function > Utility: Show message dialog**.

11   In the **Caption** of the message box, type a name to appear in the message title.

12   In the **Test of the message** box, type the text that you want the message to display.

     To display information about the settings customize the message, click **Help**.

13   In the left pane, under **Customized Requirement Script**, click **Pass**.

14   In the right pane, under **As the result of the requirement, return**, check **Fail**, and then click **OK**.

15   Click **OK**.

16   In the **Assign Policy** prompt, click **Yes**, and assign the policy to a group.

Note: One Host Integrity policy can be assigned to multiple groups, while a single group can only have a single Host Integrity policy. You can replace an existing policy with a different policy.

To test a Host Integrity policy

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

2   Under **Clients**, click and highlight the group that contains the client computers to which you applied the Host Integrity policy.

3 Under **Tasks**, click **Run a command on the group > Update Content**, and then click **OK**.

4 Log on to a client computer that runs Symantec Network Access Control and note the message box that appears.

Because the rule triggered the fail test, the message box appears. After testing, disable or delete the test policy.

See "How self enforcement works" on page 783.

See "What you can do with Host Integrity policies" on page 812.

About Host Integrity requirements

When you plan Host Integrity requirements, you must consider the following issues:

- What software (applications, files, patches, and so on) do you want to require for enterprise security?

- What occurs if a requirement is not met? For example:

  - The client can connect to a server and restore the software to meet the requirement.

  - The Host Integrity check can pass even though the requirement fails.

  - The Host Integrity check can fail and network access can be blocked.

  - A message can notify the user what to do next.

Consider the following areas in more detail:

- Which antivirus applications, antispyware applications, firewall applications, patches, or updates are required on every user's computer when it connects to the network? You usually create a separate requirement for each type of software. Predefined Host Integrity requirements let you easily set up these commonly used requirements.

- You can give users the right to select which firewall, antispyware, or antivirus applications they want to run on their computers. The predefined requirements let you specify either a specific application or a list of supported applications as acceptable. You can create a custom requirement that includes the applications that are acceptable in your company.

- How will you handle restoring a user's computer to a configuration that meets the requirements? Normally, you need to set up a remediation server with the required software. When you configure the requirement, you must specify the URL from which the client can download and install the required software.

- Some patches require a user to restart the computer. Updates are completed in a specific order so that all updates are applied before a user has to restart. As part of the Host Integrity policy, you can set the order in which requirements are checked and the remediation is tried.

- You should also consider what occurs if a requirement fails and cannot be restored. For each requirement, you have the choice to allow the Host Integrity check to pass even though that requirement fails. As part of the general Host Integrity policy, you also can configure messages. The client displays these messages to the user if the Host Integrity check fails or if it passes after previous failure. You may want to plan additional instructions for the user in these messages. In addition, you can set up a quarantine policy to activate if Host Integrity fails.
  See "Creating a Quarantine policy for a failed Host Integrity check" on page 825.

- You can simplify the management of required applications by including similar applications in one custom requirement. For example, you can include Internet browsers such as the Internet Explorer and Firefox in one requirement.

- As part of a custom requirement, you can specify whether to allow the Host Integrity check to pass if the requirement fails. When you plan how many conditions to check for in one script, remember that this setting applies to the custom requirement script as a whole. This aspect of the setting may affect whether you want to create several small custom requirements or a longer one that includes multiple steps.

You may find it helpful to set up a spreadsheet that represents your company's Host Integrity enforcement requirements.

The Host Integrity policy includes the following requirement types:

- Predefined requirements cover the most common types of Host Integrity checks and let you choose from the following types:

  - Antivirus requirement

  - Antispyware requirement

  - Firewall requirement

  - Patch requirement

  - Service pack requirement

  See "Adding Host Integrity requirements" on page 817.

- Custom requirements, which you define by using the Custom Requirement Editor.
  See "Writing a custom requirement script" on page 840.

■ Host Integrity requirement templates, which are updated as part of the Symantec Enterprise Protection LiveUpdate.
See "Adding a Host Integrity requirement from a template" on page 820.

When you add a new requirement, you can select one of the predefined requirement types. A dialog box is then displayed with the set of predefined settings that you can configure. If the predefined settings do not meet your needs, you can create a custom requirement.

You can also change the position of requirements. The position of a requirement determines the order in which it is executed.

See "Changing the sequence of Host Integrity requirements" on page 820.

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 to check

■ 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.

See "About Host Integrity requirements" on page 815.

To add a Host Integrity requirement

1 In the console, open a Host Integrity policy. (optional) Click **Overview**, and edit the **Policy name** and **Description** for the policy. Host Integrity comes with a default policy created automatically during product installation.

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 or 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 **Host Integrity Requirements** section of the dialog box, click **Add**.

6 In the **Add a Host Integrity requirement** dialog box, select one of the requirement types, and then click **OK**.

7 Configure the settings for the requirement.

See "About Host Integrity requirements" on page 815.

8 On the Advanced Settings page, configure settings for Host Integrity checks, remediation, and notifications.

For more information, click **Help**.

See "About settings for Host Integrity checks" on page 821.

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

10 Assign the policy to groups or locations.

Host Integrity for the Mac

Host Integrity for the Mac is similar to the version that is available for Windows. All choices are clearly described in the user interface.

Note: When migrating from versions of the Enforcer prior to the current one, the upgrade process does not carry over the Host Integrity policies for the Mac. You must enter them again.

Enabling, disabling, and deleting Host Integrity policies

When you create requirements for a Host Integrity policy, you can create requirements for future use. You must disable them from being used until they are needed. You can disable a requirement temporarily while you test your Host Integrity policy.

To enable and disable Host Integrity requirements

1 In the console, open a Host Integrity policy.

2 On the **Host Integrity Policy** page, click **Requirements**.

3 On the **Requirements** page, select a requirement, and then do one of the following tasks:

  ■ To enable a requirement, check the **Enable** check box for the selected requirement.

  ■ To disable a requirement, uncheck the **Enable** check box for the selected requirement.

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

To delete Host Integrity policies

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

2 Under Policies, click **Host Integrity**.

3 Select the Host Integrity policy that you want to delete from the right pane. When you select a policy it is highlighted in yellow.

4 Under **Tasks** in the left pane, click **Delete the policy**.

5 In the **Delete Policy** dialog box, click **Yes**.

Note: You cannot delete a policy that is in use. To delete a policy that is in use, you must withdraw the policy from the assigned locations first.

See "What you can do with Host Integrity policies" on page 812.

Changing the sequence of Host Integrity requirements

You can change the position of requirements. When you change the position, you determine the order in which they are executed. The position can be important when you download the software that requires a restart after installation. You set the order to ensure that the requirements that require a restart for remediation are performed last.

To change the sequence of Host Integrity requirements

1   In the console, open a Host Integrity policy.

2   On the Host Integrity page, click **Requirements**.

3   On the **Requirements** page, select the requirement that you want to move, and then click **Move Up** or **Move Down**.

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

See "Adding Host Integrity requirements" on page 817.

Adding a Host Integrity requirement from a template

You can add predefined Host Integrity requirements from existing templates. You use LiveUpdate to import the Host Integrity content into the management server and then add the templates to the Host Integrity policy.

See "Creating and testing a Host Integrity policy" on page 812.

If you import a requirement a second time and a requirement with the same name exists, the imported requirement does not overwrite the existing requirement. Instead, the imported requirement is shown with the number 2 next to its name on the Requirements table.

See "About Host Integrity requirements" on page 815.

To add a Host Integrity requirement from a template

1   In the console, open a Host Integrity policy.

2   On the **Host Integrity** page, click **Requirements**.

3   On the **Requirements** page, click **Add**.

4   In the **Add Requirement** dialog box, select one **Client platform** and **Use existing templates...**, and then click **OK**.

5   In the **Host Integrity Online Updating** dialog box, expand **Templates**, and then select a template category.

6   Next to each template you want to add, click **Add**.

7 Click **Import**.

8 Click **OK**.

About settings for Host Integrity checks

When you set up Host Integrity policies, you can select from a number of settings. The settings relate to how the Host Integrity check is carried out and how the results are handled.

See "How self enforcement works" on page 783.

If you change a Host integrity policy, it is downloaded to the client at the next heartbeat. The client then runs a Host Integrity check.

If the user switches to a location with a different Host Integrity policy while a Host Integrity check is in progress, the client stops the check. The stop includes remediation attempts, if required by the policy. The user may get a timeout message if a remediation server connection is not available in the new location. When the check is complete, the client discards the results. Then the client immediately runs a new Host Integrity check based on the new policy for the location.

If the policy is the same in the new location, the client maintains any Host Integrity timer settings. The client runs a new Host Integrity check only when required by the policy settings.

Table 43-1 displays the settings for Host Integrity checks.

Table 43-1 Host Integrity checking settings

Setting	Description
Check Host Integrity every	Specifies the frequency of Host Integrity checks.
Keep check results for	Sets the duration for maintaining Host Integrity results.
	You can set the amount of time that a client retains the result of a previous Host Integrity check. The client maintains the result even if the user takes an action that would normally result in a new Host Integrity check. For example, the user may download new software or change a location.

Table 43-1   Host Integrity checking settings *(continued)*

Setting	Description
Continue to check requirements after one fails	Specifies that the client continues to check the requirements even if one requirement fails. The client does stop the Host Integrity check until the failed requirement is restored.
	The client checks the Host Integrity requirements in the order that is specified in the Host Integrity policy.
	If you enable this setting, the Host Integrity check fails, but you can try other remediation actions, if required.
	You can allow the Host Integrity check to pass even if a requirement fails. This setting is found on the **Requirements** dialog box for each requirement type. You apply the setting separately for each requirement.

Allowing the Host Integrity check to pass if a requirement fails

In addition to enabling or disabling a requirement on your Host Integrity policy to determine whether or not the client runs the requirement script, you can have the client run the requirement script and log the results but ignore the results. You can let the Host Integrity check pass whether or not the requirement fails. A requirement can pass even if the requirement condition is not met.

You enable **Allow the Host Integrity check to pass** even if the requirement fails on the dialog for a specific requirement. If you want to apply this setting to all requirements, you must enable the setting on each requirement separately. The setting is disabled by default.

If you enable the setting to allow the Host Integrity check to pass even if the requirement fails, the following message appears in the client window when the event occurs:

```
Host Integrity failed but reported as pass
```

To allow the Host Integrity check to pass if a requirement fails

1   In the console, open a Host Integrity policy.

2   On the **Host Integrity** page, click **Requirements**.

3   On the **Requirements** page, click **Add**, add a predefined requirement or a custom requirement, and then click **OK**.

4   On the dialog box for the requirement, check **Allow the Host Integrity check to pass even if this requirement fails**.

5   Click **OK**.

6   When you finished with the configuration of this policy, click **OK**.

See "Adding Host Integrity requirements" on page 817.

Configuring notifications for Host Integrity checks

When the client runs a Host Integrity check, you can configure notifications to appear when the following conditions occur:

■   A Host Integrity check fails.

■   A Host Integrity check passes after it previously failed.

The results of the Host Integrity check appear in the client's Security log. They are uploaded to the Compliance log on the **Monitors** page of the management server.

The client's Security log contains several panes. If you select a Host Integrity check event type, the lower-left pane lists whether the individual requirement has passed or failed. The lower right-hand pane lists the conditions of the requirement. You can configure the client to suppress the information in the lower right-hand pane. Although you may need this information when troubleshooting, you may not want users to view the information. For example, you may write a custom requirement that specifies a registry value or a file name. The details are still recorded in the Security log.

You can also enable a notification that gives the user the choice to download the software immediately or postpone the remediation.

See "Allowing users to postpone or cancel Host Integrity remediation" on page 827.

To configure notifications for Host Integrity checks

1   In the console, open a Host Integrity policy.

2   On the **Host Integrity** page, click **Advanced Settings**.

3   On the **Advanced Settings** page, under **Notifications**, to show detailed requirement information, check **Show verbose Host Integrity Logging**.

The lower right-hand pane of the client's Security log displays complete information about a Host Integrity requirement.

4   Check any of the following options:

■   **Display a notification message when a Host Integrity check fails**.

- ■ **Display a notification message when a Host Integrity check passes after previously fails**.

5   To add a custom message, click **Set Additional Text**, type up to 512 characters of additional text, and then click **OK**.

6   When you are finished with the configuration of this policy, click **OK**.

About Host Integrity remediation

If the client Host Integrity check shows that the Host Integrity requirements are not met, the client can try to restore the necessary files to meet the requirements The client computer then needs to pass the Host Integrity check. The client downloads, installs files, or runs required applications. When you set up Host Integrity Policies, you can specify what happens during the remediation process. You can specify not only where the client goes to download remediation files but also how the remediation process is implemented.

You can allow the user to cancel software being downloaded. You can also set the number of times the user can postpone a download and for how long. The settings apply to all types of requirements in the policy except those on which you have disabled remediation cancellation. Users can cancel predefined requirements only.

See "About remediating applications and files for Host Integrity" on page 824.

About remediating applications and files for Host Integrity

When you set up remediation for a requirement, you specify the location of an installation package or files to be downloaded and installed.

See "About Host Integrity remediation" on page 824.

When you specify the location of the installation package or file to be downloaded, you can use any of the following formats:

UNC	\\servername\sharename\dirname\filename
	UNC restore does not work if Network Neighborhood browsing is disabled on the target client. Be certain that Network Neighborhood browsing has not been disabled if you use UNC paths for remediation.
FTP	FTP://ftp.ourftp.ourcompany.com/folder/filename
HTTP	HTTP://www.ourwww.ourcompany.com/folder/filename

Installation packages or files are always downloaded to the temporary directory. Any relative path refers to this directory. The temporary directory is defined in the TMP environment variable if it exists, or in the TEMP environment variable if that exists. The default directory is in the Windows directory.

For file execution, the current working directory is always set to the Windows temporary directory. Environment variables are substituted before execution. The Windows directory path replaces the command %windir%.

You can use %F% (the default) to execute the file you specified in the Download URL field. The `%F%` variable represents the last downloaded file.

After the download, installation, or execution of a command to restore a requirement, the client always retests the requirement. Also, the client logs the results as pass or fail.

Host Integrity remediation and Enforcer settings

When you set up Host Integrity requirements, you can specify that if the Host Integrity requirements are not met, the client should update the client computer with whatever is required by connecting to a remediation server. If you apply such requirements to clients that connect to the network through an Enforcer, you must ensure that the client, while blocked from regular network access, can access the remediation server. Otherwise, the client does not restore Host Integrity and the client continues to fail the Host Integrity requirement.

How you accomplish this task depends on the type of Enforcer. The following list offers a few examples:

- For the Gateway Enforcer, you can configure the Gateway Enforcer to recognize the remediation server as a trusted internal IP address.

- For a LAN Enforcer, if you use a switch with dynamic VLAN capability, you can set up a VLAN with access to the remediation server.

See "About Host Integrity remediation" on page 824.

Creating a Quarantine policy for a failed Host Integrity check

The Quarantine policy is a policy for the Symantec Network Access Control client that runs the Host Integrity check. If the Host Integrity policy requirements are not met, the client tries remediation. If remediation fails, the client automatically switches to a Quarantine policy. A Quarantine policy can be any of the existing policies, such as the Virus and Spyware Protection policy or the Firewall policy.

You can set up and assign a Quarantine policy to a location.

To create a Quarantine policy for a failed Host Integrity check

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

2   On the **Clients** page, under **Clients**, select the group for which you want to create a policy.

3   On the **Policies** tab next to **Quarantine Policies when Host Integrity Fails**, click **Add a policy**.

4   In the **Add Quarantine Policy** dialog box, choose a policy type and then click **Next**.

5   Choose whether to add an existing policy, create a new policy, or import a policy file, and then click **Next**.

6   Do one of the following tasks:

   ■ In the **Add Policy** dialog box, choose the policy, and click **OK**.

   ■ In the **Policy Type** dialog box, configure the policy, and click **OK**.

   ■ In the **Import Policy** dialog box, locate the .dat file and click **Import**.

See "About Host Integrity remediation" on page 824.

See "About Host Integrity requirements" on page 815.

Specifying the amount of time the client waits to remediate

You can specify the amount of time the client waits before it tries to install and start the remediation download again. Regardless of the time that you specify, whenever a new Host Integrity check is initiated, the client tries to remediate the client computer again.

To specify the amount of time the client waits to remediate

1   In the console, open a Host Integrity policy.

2   On the **Host Integrity Policy** page, click **Requirements**.

3   On the **Requirements** page, click **Add**, add a predefined requirement, and then click **OK**.

4   On the dialog box for each predefined requirement, check **Install** *requirement name* **if it has not been installed on the client**.

5   Check **Download Installation Package**.

   For the Antivirus requirement, check **Download the installation package**.

6   Check **Specify wait time before attempting the download again if the download fails**.

7   Specify the amount of time to wait by the minutes, hours, or days.

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

See "About Host Integrity remediation" on page 824.

Allowing users to postpone or cancel Host Integrity remediation

If a requirement specifies a remediation action, you can allow the user to cancel the remediation. Or, you can allow the user to postpone the remediation to a more convenient time. Examples of remediation actions include the installation of an application or an update of a signature file. You can set a limit on how many times a remediation can be canceled and how long the user can postpone it. The limits you set determine the selections available to the user on the message window that the client displays when remediation is needed. You can also add text to the message window.

The minimum and the maximum time settings determine the range of choices available on the message window. The message window displays to a user when a requirement fails. The range appears as a list next to the Remind me later icon on the message.

If the user selects a shorter time for postponement than the Host Integrity check frequency, the user selection is overridden. The message window does not appear again until the client runs another Host Integrity check. If the user has chosen to be reminded in 5 minutes, but the Host Integrity check runs every 30 minutes, the remediation message window does not appear until 30 minutes have passed. To avoid confusion for the user, you may want to synchronize the minimum time setting with the Host Integrity check frequency setting.

If the user postpones remediation, the client logs the event. The Host Integrity is shown as failed since the requirement is not met. The user can manually run a new Host Integrity check at any time from the client user interface.

If the user has postponed a remediation action and in the interim the client receives an updated policy, the amount of time available for remediation is reset to the specified maximum.

To allow users to postpone Host Integrity remediation

1   In the console, open a Host Integrity policy.

2   On the **Host Integrity Policy** page, click **Advanced Settings**.

3   On the **Advanced Settings** page, under **Remediation Dialog Options**, set a minimum time limit and the maximum time limit that a user can postpone the remediation.

4   Type the maximum number of times that the user can cancel the remediation.

5   To add a custom message on the client computer, click **Set Additional Text**.

     The message you type is displayed on the client remediation window if the user clicks the **Details** option. If you specify no additional text, the default window text is repeated in the Details area when the user clicks Details.

6   In the **Enter Additional Text** dialog box, type a custom message up to 512 characters, and then click **OK**.

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

To allow users to cancel Host Integrity remediation

1   In the console, open a Host Integrity policy.

2   On the **Host Integrity Policy** page, click **Requirements**.

3   On the **Requirements** page, click **Add**, add a predefined requirement, and then click **OK**.

4   On the dialog box for each predefined requirement, check **Install** *requirement name* **if it has not been installed on the client**.

5   Check **Download Installation Package**.

     For the Antivirus requirement, check **Download the installation package**.

6   Check **Allow the user to cancel the download for Host Integrity remediation**.

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

See "About Host Integrity remediation" on page 824.

Chapter 44

Adding custom requirements to a Host Integrity policy

This chapter includes the following topics:

About custom requirements

Custom requirements check a client computer for any number of administrator-selected or defined criteria. You can write custom requirements to remediate any identified compliancy issues.

You can create a complex or a simple requirement script by using predefined selections and fields.

The fields and lists that are available in the predefined requirement dialog boxes are available when you create custom requirements. However, custom requirements give you more flexibility. In custom requirements, you can add the applications that are not included in the predefined lists of applications. You can create subsets of predefined lists by adding each application individually.

See "About conditions" on page 830.

See "About functions" on page 836.

See "About custom requirement logic" on page 838.

About conditions

Conditions are the checks that may be performed within a custom requirement script to detect compliancy issues.

You can choose from the following categories of conditions:

- Virus protection checks
  See "About antivirus conditions" on page 831.

- Spyware protection checks
  See "About antispyware conditions" on page 831.

- Firewall checks
  See "About firewall conditions" on page 832.

- File checks and operation
  See "About file conditions" on page 832.

- Registry checks and operations
  See "About registry conditions" on page 835.

- Utilities

You can specify conditions as present or absent (NOT). You can include multiple condition statements by using AND or OR keywords.

About antivirus conditions

In a custom requirement, you can specify virus protection applications and signature file information to check as part of your IF-THEN condition statement.

You can check for the following conditions:

- Virus protection is installed

- Virus protection is running

- Virus protection signature file is up to date

- Virus protection has not reported an infection. This applies only to Windows computers, and only if Symantec Endpoint Protection is the antivirus program. If you select this condition, only Symantec Endpoint Protection can be specified as the antivirus program.

When you check applications and signature files as part of a custom requirement, you specify the same information as when you create a predefined requirement. The option names may differ slightly.

If you select **Any Antivirus Product**, any of the applications in the drop-down list meet the requirement. You can include a subset of applications by selecting each by using the OR keyword.

When you specify the signature file information, you can select one or both options for checking that the signature file is up to date. If you select both, the following conditions must be satisfied to meet the requirement:

- Select **Check signature file is less than** and enter a number of days.
  A file that is dated before the number of days you specify is out of date.

- Select **Check signature file date is** and select **before**, **after**, **equal to**, or **not equal to**, and specify a date in the form "mm/dd/yyyy." Optionally, specify an hour and minute; the default is 00:00. The file's last modified date determines the signature file age.

See "Adding Host Integrity requirements" on page 817.

About antispyware conditions

For a custom Host Integrity requirement, you can specify antispyware applications and signature file information to check as part of your IF THEN condition statement.

You can check for the following conditions:

- An antispyware application is installed

- Antispyware is running

■ The antispyware signature file is up to date

When you check applications and signature files as part of a custom requirement, you can specify the same information as when you create a predefined requirement. The option names may differ slightly.

If you select **Any Antispyware Product**, any of the applications in the drop-down list meet the requirement.

When you specify the signature file information, you can select one or both options for checking that the signature file is up to date. If you select both options, both of the following conditions must be satisfied to meet the requirement:

■ Select **Check signature file** to specify the age of the file. Enter a number of days that is the maximum age of the file.
A file that is dated before the number of days you specify is out of date.

■ Select **Check signature file date is less than** and select **before**, **after**, **equal to**, or **not equal to**, and specify a date in the form "mm/dd/yyyy." Optionally, specify an hour and minute; the default is 00:00. The file's last modified date determines the signature file age.

See "Adding Host Integrity requirements" on page 817.

About firewall conditions

For a custom Host Integrity requirement, you can specify firewall applications to check as part of your IF-THEN condition statement.

You can check for the following conditions:

■ Firewall is installed

■ Firewall is running

If you want to select any of the applications in the drop-down list, you can select **Any Firewall Product**. You can include a subset of applications by selecting each using the OR keyword.

See "Adding Host Integrity requirements" on page 817.

About file conditions

For a custom Host Integrity requirement, you can check an application or a file as part of your IF-THEN condition statement.

You can specify the following options to check file information in a custom Host Integrity requirement:

File: Compare file age to	Specify a number of days or weeks and select greater than or less than.
File: Compare file date to	Specify a date in the format mm/dd/yyyy. Optionally, specify an hour and minute. The default time is 00:00. You can select equal to, not equal to, before, or after.
File: Compare file size to	Specify the number of bytes. You can select equal to, not equal, less than, or greater than.
File: Compare file version to	Specify a file version in the format x.x.x.x, where x represents a decimal number from 0 to 65535. You can select equal to, not equal, less than, or greater than.
File: File exists	Specify the name of the file to be checked for.
File: File fingerprint equals	Normally you get this information by selecting an application using **Search for Applications**. You must specify the file fingerprint.
	Note: You can search for the file fingerprint from a list of client computers.
Specify a hexadecimal number (up to 32 digits)	When you select an option, additional fields appear on the dialog. For each option you specify the file name and path and you enter the additional information that is required.
File: File download complete	You can download a file from a location that you specify to a directory that you specify, downloading by FTP or UNC or HTTP. If authentication is required to access a file location, you can specify the user name and password.
	Note: If you want users to download the file from an FTP or UNC file share, you must set up the share folder or FTP server to allow anonymous access.

You can use system variables, registry values, or a combination of them to specify the file name and path. When you select one of the file options, the dialog shows examples of ways to enter the file name and path.

You can locate the applications that have been recorded by using the Search for Applications feature. When you specify file options in the custom requirement script, the **Search for Applications** option provides access to the same search tool as the **Search for Applications** tool. You can browse the groups that are defined in the management server to filter applications, enter a search query, and export the results to a file.

To search using system environment variables or registry values:

To use the system environment variable	To specify the file named cmd.exe located under the directory that is specified in the WINDIR environment variable, type the following command: `%WINDIR%\cmd.exe`
To use the registry value	To read the value `HKEY_LOCAL_MACHINE\Software\` `Symantec\\AppPath` as the path of the file `sem.exe`, type the following command: `#HKEY_LOCAL_MACHINE\Software\Symantec\AppPath#\sem.exe`
To use the combined registry and system environment variable	Use the following example to use the combined registry value and system environment variable: `%SYSTEMDIR%\#HKEY_LOCAL_MACHINE\Software\Symantec\\AppPath#.`

See

About operating system conditions

For a custom Host Integrity requirement, you can specify operating system information to check as part of your IF-THEN condition statement. When you select an option, additional fields appear on the dialog.

Utility: Operating system is	Specify an operating system. When you want to update a patch, you need to select the exact versions that require that patch. You can use the OR keyword to specify more than one operating system.
Utility: Operating system language is	The function detects the language version of the client's operating system. If the language version is not listed in the **Custom Requirement** dialog, you can add languages by typing their identifiers in the **Language Identifiers** field. To add multiple identifiers, use a comma to separate each ID such as 0405,0813. See the Language Identifiers table in context-sensitive Help for the list of identifiers.

Patch: Compare current service pack with specified version	Type the number of the service pack that you want to check for, such as 2. The number is limited to two characters. You can check for the following conditions: **equal to**, **not equal to**, **less than**, or **greater than**.
	A number that is followed by a letter is considered greater than the number alone; for example, service pack number 6a is considered greater than 6. Be sure to apply patches one at a time.
Patch: Patch is installed	Type the patch name that you want to check for. For example: KB12345. You can type only numbers and letters in this field.

Be sure to match the patch name or service pack number with the correct version of the operating system. If you specify an operating system that does not match the patch or the service pack, the requirement fails.

See "Adding Host Integrity requirements" on page 817.

About registry conditions

For a custom Host Integrity requirement, you can specify Windows registry settings to check as part of your IF-THEN condition statement. You can also specify ways to change registry values. Only HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, and HKEY_CURRENT_CONFIG are supported registry settings

The following selections are available for checking registry settings:

Registry: Registry key exists	Specify a registry key name to check whether it exists.
Registry: Registry value equals	Specify a registry key name and a value name and specify what data to compare the value against.
Registry: Registry value exists	Specify a registry key name to check if it has the specified value name.
Registry: Set registry value successful	Specify a value to assign for the specified key; if the key does not exist, it creates the key. This selection replaces an existing value, whether or not it is of the same type. If the existing value is a DWORD value but you specify a string value, it replaces the DWORD with the string value.

Registry: Increment registry DWORD value successful	Specify a DWORD value. This selection lets you perform counts, such as allowing an unpatched computer to meet the requirement no more than n times.

When you specify registry keys, remember the following considerations:

- The key name is limited to 255 characters.

- If the registry key has a backslash (\) at the end, it is interpreted as a registry key. For example: `HKEY_LOCAL_MACHINE\SOFTWARE\`

- If the registry key has no backslash at the end, then it is interpreted as a registry name. For example: `HKEY_LOCAL_MACHINE\SOFTWARE\ActiveTouch`

When you specify registry values, remember the following considerations:

- The value name is limited to 255 characters.

- You can check for values as DWORD (decimal), Binary (hexadecimal), or String.

- For DWORD values, you can check whether the value is less than, equal to, not equal to, or greater than the specified value.

- For String values, you can check whether the value data equals or contains a given string. If you want the string comparison to be case sensitive, check the Match case check box.

- For Binary values, you can check whether the value data equals or contains a given piece of binary data. Hexadecimal bytes represent the data. If you specify value contains, you can also specify the offset for this data. If the offset is left blank, it searches the value for the given binary data. Allowed values for the hexadecimal edit box are 0 through 9 and a through f.

The following are examples of registry values:

DWORD	12345 (in decimal)
Binary	31 AF BF 69 74 A3 69 (in hexadecimal)
String	ef4adf4a9d933b747361157b8ce7a22f

See "Adding Host Integrity requirements" on page 817.

About functions

You use functions to define the actions that are performed when a conditional expression is evaluated as true or false.

A custom requirement condition can check for the installation of a particular antivirus product, but it cannot be configured to install the product as a remediation action. When you write custom requirements, you must explicitly define the remediation actions to be performed by using function statements.

Functions appear within THEN and ELSE statements, or may appear at the top or end of a custom requirement script. To achieve a desired remediation result, you may need to specify multiple functions. Each function performs a very specific task, such as to download a file or to execute a file. You do not define individual functions to provide specific remediation actions, such as to install a specific antivirus product. To download a specific antivirus product, you must use the general download function.

Table 44-1 displays the following functions in a custom requirement script:

Table 44-1   Custom requirement functions

Function	Description
Download a file	Downloads a file that is referenced by a URL or UNC to the client computer. If a URL is used, both HTTP and FTP are supported.
Set registry value Increment registry DWORD value	Creates and then sets or increments a Windows registry value within a specified registry key.
Log message	Specifies a custom message to be added to the client Security log and the registry.
Run a program	Executes a program that is already resident on the client computer. You can specify the program to run whether or not the user is logged on.
Run a script	Runs a custom script on the client computer. You can use the built-in text editor to create the script contents. The script may be a batch file, an INI file, or any executable format Windows recognizes. Additionally, the script may contain only parameters to be provided to another program.
Set Timestamp	Stamps a specified file on the client computer with the current time and date.
Show message dialog	Displays a message dialog window on the client computer with an OK option. A default timeout may be specified.
Wait	Pauses the execution of the custom requirement script for a specified period.

See "Adding Host Integrity requirements" on page 817.

About custom requirement logic

You write the custom requirements by using the script-like logic. The rules use IF..THEN..ELSE logic from a list of predefined conditions and actions.

See "About the RETURN statement" on page 838.

See "About the IF, THEN, and ENDIF statement" on page 838.

See "About the ELSE statement" on page 839.

See "About the NOT keyword" on page 839.

See "About AND, OR keywords" on page 839.

About the RETURN statement

You can add a RETURN statement to specify the overall Host Integrity result of the requirement. The RETURN statement includes the PASS keyword and the FAIL keyword. All custom requirements must include a RETURN statement at the end.

Unlike a predefined requirement, a custom requirement must explicitly specify the result of the Host Integrity check. In some cases, the evaluation of a set of conditions as being true should be interpreted as the custom requirement passing Host Integrity evaluation. In other cases, you may want the same evaluation to be interpreted as failing Host Integrity evaluation.

See "Adding Host Integrity requirements" on page 817.

About the IF, THEN, and ENDIF statement

You can define the primary logic structure of a custom requirement by one or more IF, THEN, and ENDIF statements. An IF, THEN, and ENDIF statement:

■ Defines a structure in which specific conditions are checked (IF).

■ The actions that are taken when those conditions are evaluated as being true (THEN).

You can nest IF, THEN, and ENDIF statements to form more complex custom requirements. You must nest the IF, THEN, and ENDIF statements whenever one condition must be true before another condition can be evaluated.

See "Adding an IF THEN statement" on page 841.

About the ELSE statement

An IF, THEN, and ENDIF statement is a set of conditions and actions that are executed when the conditions are evaluated as being true. In many cases, you may need to specify one or more actions to be taken to perform a desired remediation action. You may add an ELSE statement to identify the actions to be taken whenever the specified conditions are evaluated as being false.

See "Adding an ELSE statement" on page 842.

About the NOT keyword

You can use the NOT keyword to reverse the logical evaluation of a particular condition. After a condition has been added to the custom requirement script, right-click the condition and select Toggle NOT to reverse the logical of the condition. The use of the NOT keyword does not change the overall true and false evaluation of the IF statement. It reverses only the true and the false state of a particular condition.

See "Adding Host Integrity requirements" on page 817.

About AND, OR keywords

You can specify multiple conditions within an IF, THEN, or ENDIF statement; however, additional keywords must be added to the statement. Within any IF statement, you can add the AND OR keywords to logically associate multiple conditions. The logical association of the conditions directly affects the overall true or false evaluation of the IF statement. If you use the AND keyword in an IF statement, all the conditions in the IF statement must be evaluated as true for the IF statement to be true. If you use the OR keyword, only one of the conditions in the IF statement must be evaluated for the IF statement to be true.

When you specify multiple conditions, you must interpret the logical association of the conditions to anticipate what the correct true or false evaluation should be. The custom requirement script does not display the expression with a parenthesis format, but with nested keywords and nodes. The first expression always begins with the first condition specified, and continues as long as the same logical operator keyword is used. For example, you can use the OR keyword to associate three different conditions. As long as you use the OR keyword, all the conditions are contained within the same logical expression.

See "Adding Host Integrity requirements" on page 817.

Writing a custom requirement script

To build a custom requirement, you add one or more IF..THEN.. statements to a script. When you run the script, the Host Integrity check looks for the condition that is listed under the IF node. Depending upon the condition, the action that is listed under the THEN node is executed. The result (pass or fail) is returned.

The script displays a tree structure in the left pane and a drop-down list of conditions or functions in the right pane.

As part of a custom requirement, you can specify whether to allow the Host Integrity check to pass if the requirement fails. When you plan how many different conditions to check for in one script, remember that this setting applies to the entire custom requirement script. This choice may affect whether you want to create several small custom requirements or a longer one that includes multiple steps.

To write a custom requirement script

1   Add a custom requirement.

    See "Adding Host Integrity requirements" on page 817.

2   In the **Custom Requirement** dialog box, type a name for the requirement.

    The requirement name can appear on the client computer. The name notifies the user whether the requirement has passed or the requirement has failed or prompts the user to download the software.

3   To add a condition, under **Customized Requirement Script**, click **Add**, and then click **IF..THEN..**.

4   With the highlight on the empty condition under the IF node, in the right pane, select a condition.

    The Host Integrity check looks for the condition on the client computer.

5   Under the **Select a condition** drop-down list, specify the additional information that is required.

6   Under **Customized Requirement Script,** click THEN, and then click **Add**.

    The THEN statement provides the action that should be taken if the condition is true.

7   Click any of the following options:

    ■   IF.. THEN
        Use a nested IF.. THEN.. statement to provide additional conditions and actions.
        See "Adding an IF THEN statement" on page 841.

- Function
  Use a function to define a remediation action.
  See "About functions" on page 836.

- Return
  Use a return statement to specify whether the results of the evaluation of the condition passes or fails. Every custom requirement must end with a pass or fail statement.

- Comment
  Use a comment to explain the functionality of the conditions, functions, or statements that you are adding.
  See "Adding a comment" on page 842.

8   In the right-hand pane, define the criteria that you added.

    For more information on these options, click **Help**.

9   To add more nested statements, conditions, or functions, under **Customized Requirement Script**, right-click the node, and then click **Add**.

10 Repeat steps 7 to 9 as needed.

11 To allow the Host Integrity check to pass no matter what the result, check **Allow the Host Integrity check to pass even if this requirement fails**.

12 When you are done with the configuration of the requirement, click **OK**.

Adding an IF THEN statement

Add an IF..THEN statement to a custom script to define conditions to check and actions to take if the condition is evaluated as true.

To add an IF THEN statement

1   Write a custom requirement script.

    See "Writing a custom requirement script" on page 840.

2   Under **Customized Requirement Script**, select one of the following:

    - To add the first IF THEN statement, select the top node.

    - To add an IF THEN statement at the same level as an existing one, select **END IF**.

    - To add a nested IF THEN statement, select the line under which you want to add it.

3   Click **Add**.

4   Click **IF..THEN**.

Switching between the IF statement and the IF NOT statement

You may need to change between checking for the presence or absence of a condition.

To change between the IF statement and the IF NOT statement

1   Write a custom requirement script.

    See "Writing a custom requirement script" on page 840.

2   Right-click the condition, and then click **Toggle NOT**.

Adding an ELSE statement

You may add an ELSE statement to identify the actions to be taken whenever the specified conditions are evaluated as being false.

To add an ELSE statement

1   Write a custom requirement script.

    See "Writing a custom requirement script" on page 840.

2   Under **Customized Requirement Scrip**t, click **THEN**.

3   Click **Add**, and then click **ELSE**.

Adding a comment

For informational purposes, you can choose to add a comment to a statement.

To add a comment

1   Write a custom requirement script.

    See "Writing a custom requirement script" on page 840.

2   Under **Customized Requirement Script**, select any statement that you have already added, and then click **Add**.

3   Click **Comment**.

4   Click **//Insert statements here**, and in the right-hand pane, in the **Comment** text field, enter your comments.

Copying and pasting IF statements, conditions, functions, and comments

You can copy and paste statements or entire IF THEN nodes within or between custom requirements. You may want to copy and paste these elements if you want to move them to another part of the script or to repeat the functionality.

To copy and paste an IF statement

1 Write a custom requirement script.

See "Writing a custom requirement script" on page 840.

2 Under **Customized Requirement Script**, right-click the script element, and then click **Copy**.

3 Right-click an empty statement line, and then click **Paste**

Deleting a statement, condition, or function

You can delete statements, conditions, or functions at any time. If there is only one condition statement under an IF node, deleting it deletes the entire IF THEN statement.

To delete a statement, condition, or function

1 Write a custom requirement script.

See "Writing a custom requirement script" on page 840.

2 Under **Customized Requirement Script**, select the requirement element that you want to delete.

3 Click **Delete**.

4 If you are asked to confirm the deletion, click **Yes**.

Displaying a message dialog box

You can specify a function or a condition in the custom Host Integrity requirement that creates a message that the client displays to the user. The function or the condition returns true if the user clicks OK or Yes. Otherwise it returns false.

To display a message dialog box

1 Write a custom requirement script.

See "Writing a custom requirement script" on page 840.

2 In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.

3 Click **Add**, and then click **Function**.

4 Click **Utility: Show message dialog**.

To insert a condition, select **IF...Then**, and then select the appropriate branch. Then select **Utility: Message dialog return value equals**.

5 Type a caption for the message box, up to 64 characters.

6 Type the text for the message box up, to 480 characters.

7 Select one of the following icons to display: Information, Question, Warning, or Error.

Both the icon and the text appear.

8 Select the set of options that appear in the dialog box:

- OK

- OK and Cancel

- Yes and No

9 Select the default option for each set of options.

10 To close the message box and return a default value after a certain time with no user interaction, check **Action to take to dismiss message box after maximum waiting time**, and specify the wait time.

The time value must be greater than 0.

Downloading a file

For a custom requirement, you can specify that a file is downloaded to the client computer.

To download a file

1 Write a custom requirement script.

See "Writing a custom requirement script" on page 840.

2 In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.

3 Click **Add**, and then click **Function**.

4 Click **File: Download a file**.

5 Enter the URL location that the file is downloaded from, and the folder on the client computer you want the file to be downloaded to.

You can specify the location by a URL or a UNC. If you use a URL, both HTTP and FTP are supported.

If you choose HTTP, check **Authentication required for HTTP only**. Enter the user name and password for the authentication.

6 Check **Show the download process dialog** so that the users can watch the file as the file gets downloaded to the client computer.

7 If you want the user to be able to cancel the file download, check **Allow the user to cancel Host Integrity for this requirement**.

Users may lose work if the file is downloaded at the wrong time.

Setting a registry value

For a custom requirement, you can set a Windows registry value to a specific value. The Set registry value function creates the value if it does not already exist.

To set a registry value

1 Write a custom requirement script.

See "Writing a custom requirement script" on page 840.

2 In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.

3 Click **Add**, and then click **Function**.

4 Click **Registry: Set registry value**. The registry value contains the value name and type to be checked.

5 Enter the registry key in the **Registry key** field.

6 Enter a value name to be checked in the **Value name** field.

7 Under **Specify Type and Data**, choose one of the following value and content types:

- DWORD value
- String value
- Binary value

Incrementing a registry DWORD value

For a custom requirement, you can increment the Windows registry DWORD value. The Increment registry DWORD value function creates the key if it does not exist.

To increment the registry DWORD value

1   Write a custom requirement script.

    See "Writing a custom requirement script" on page 840.

2   In the **Custom Requirement** dialog box, under **Customized Requirement Script** , select the node where you want to add the function.

3   Click **Add**, and then click **Function**.

    Click **Registry: Increment registry DWORD value**.

4   Enter the registry key to check in the **Registry key** field.

5   Enter a value name to be checked in the **Value name** field.

Running a program

For a custom Host Integrity requirement, you can specify a function to have the client launch a program.

To run a program

1   Write a custom requirement script.

    See "Writing a custom requirement script" on page 840.

2   In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.

3   Click **Add**, and then click **Function**.

4   Click **Utility: Run a program**.

5   In the command text field, type the command to execute the script.

    Environment variables are substituted before execution. For example, %windir% replaces the Windows directory path.

6   Under **Run the Program**, select one of the following options:

    ■ in system context

    ■ in logged-in user context
      The Execute command must include the whole file path, thus showing who the logged-in user is. If no user is logged in, the result fails.

7   To specify the amount of time to allow the execute command to complete, select one of the following options:

    ■ Do not wait
      The action returns true if the execution is successful but it does not wait until the execution is completed.

- Wait until execution completes

- Enter maximum time
  Enter a time in seconds. If the Execute command does not complete in the specified time, the file execution is terminated.

8   Optionally, uncheck **Show new process window** if you do not want to see a window that shows the requirement running the program.

Running a script

In the custom Host Integrity requirement, you can specify a function that causes the client to run a script. You can use a scripting language, such as JScript or VBScript, which you can run with the Microsoft Windows Script Host.

To run a script

1   Write a custom requirement script.

   See "Writing a custom requirement script" on page 840.

2   In the **Custom Requiremen**t dialog box, under **Customized Requirement Script**, select the node where you want to add the function.

3   Click **Add**, and then click **Function**.

4   Click **Utility: Run a script**.

5   Enter a file name for the script, such as myscript.js.

6   Type the content of the script.

7   In the **Execute the command** text field, type the command to execute the script.

   Use %F to specify the script file name. The script executes in system context.

8   To specify the amount of time to allow the execute command to complete, select one of the following options:

- Do not wait
  The action returns true if the execution is successful but it does not wait until the execution is completed.

- Wait until execution completes

- Enter maximum time
  Enter a time in seconds. If the Execute command does not complete in the specified time, the file execution is terminated.

9   Optionally uncheck **Delete the temporary file after execution is completed or terminated** if you no longer need it.

This option is disabled and unavailable if Do not wait is selected.

10   Optionally uncheck **Show new process window** if you do not want to see a window that shows the requirement running the script.

Setting the timestamp of a file

In the custom Host Integrity requirement, you can specify the Set Timestamp function to create a Windows registry setting to store the current date and time. You can then use the Check Timestamp condition to find out if a specified amount of time has passed since that timestamp was created.

For example, if the Host Integrity check runs every 2 minutes, you can specify an action to occur at a longer interval such as a day. In this case, the stored time value is removed:

■   When the client receives a new profile.

■   When the user manually runs a Host Integrity check.

To set the timestamp of a file

1   Write a custom requirement script.

See "Writing a custom requirement script" on page 840.

2   In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.

3   Click **Add**, and then click **Function**.

4   Click **Utility: Set Timestamp**.

5   Type a name up to 256 characters long for the registry setting that stores the date and the time information.

To compare the current time to the stored time value

1   Write a custom requirement script.

See "Writing a custom requirement script" on page 840.

2   In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the condition.

3   Click **Add**, and then click **IF..THEN...**.

4   Click **Utility: Check Timestamp**.

5 Type the name you entered for the saved time registry setting.

6 Specify an amount of time in minutes, hours, days, or weeks.

If the specified amount of time has passed, or if the value of the registry setting is empty, the Set Timestamp function returns a value of true.

Specifying a wait time for the custom requirement script

In the custom Host Integrity requirement, you can specify a function that causes the custom requirement script to wait for a specified length of time before it runs.

To specify a wait time for the script

1 Write a custom requirement script.

See "Writing a custom requirement script" on page 840.

2 In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.

3 Click **Add**, and then click **Function**.

4 Click **Utility: Wait**.

5 Type the number of seconds to wait.

Performing basic tasks on the console of all types of Enforcer appliances

This chapter includes the following topics:

- About performing basic tasks on the console of an Enforcer appliance
- Configuring a connection between an Enforcer appliance and a Symantec Endpoint Protection Manager
- Checking the communication status of an Enforcer appliance on the Enforcer console
- Remote access to an Enforcer appliance
- About the Enforcer appliance CLI command hierarchy

About performing basic tasks on the console of an Enforcer appliance

You must have already configured the following parameters during the installation of the Enforcer appliance:

- Host name of the Enforcer appliance
- Group name of the Enforcer appliance group of which a particular Enforcer appliance is a member
- IP addresses of the internal and the external network interface cards (NICs)
- IP address of the DNS server, if applicable

- IP address of the NTP server, if applicable

However, you must still configure a connection between an Enforcer appliance and a Symantec Endpoint Protection Manager. You execute the spm command on the console of the Enforcer appliance to configure this connection. You cannot proceed to use an Enforcer appliance unless you complete this task.

See "Configuring a connection between an Enforcer appliance and a Symantec Endpoint Protection Manager" on page 852.

After initially installing and configuring an Enforcer appliance, you can perform administrative tasks from the Enforcer console or Symantec Endpoint Protection Manager. If you administer multiple Enforcer appliances, it is convenient to administer them all from one centralized location

All Enforcer appliances also have a command-line interface (CLI) from which you can execute commands to change any number of parameters.

See "About the Enforcer appliance CLI command hierarchy" on page 855.

Configuring a connection between an Enforcer appliance and a Symantec Endpoint Protection Manager

You must establish communication between the Enforcer appliance and the Symantec Endpoint Protection Manager on the Enforcer console. You must have also completed the installation of the Enforcer appliance and the configuration of the internal and the external NICs on the Enforcer appliance.

See "About installing an Enforcer appliance" on page 800.

If you want to establish communication between an Enforcer appliance and the Symantec Endpoint Protection Manager on an Enforcer console, you need the following information:

- IP address of the Symantec Endpoint Protection Manager
  Check with the administrator of the server on which the Symantec Endpoint Protection Manager has been installed to obtain the IP address.

- Enforcer group name to which you want to assign the Enforcer appliance
  After you finish configuring the Enforcer group name for the Enforcer appliance, the group name automatically registers on the Symantec Endpoint Protection Manager.

- Port number on the Symantec Endpoint Protection Manager that is used to communicate with the Enforcer appliance.
  The default port number is 8014.

- The encrypted password that was created during the initial installation of the Symantec Endpoint Protection Manager.

To configure a connection between an Enforcer appliance and a Symantec Endpoint Protection Manager

1   At the command line on the console of an Enforcer appliance, type `configure`.

2   Type the following command:

    `spm ip` *ipaddress* `group` *Enforcer group name* `http` *port number* `key` *encrypted password*

    See "configure spm" on page 853.

    You can use the following example as a guideline:

    `spm ip` *192.168.0.64* `group` *CorpAppliance*
    `http` *8014* `key` *symantec*

    This example configures the Enforcer appliance to communicate with the Symantec Endpoint Protection Manager that has an IP address 192.168.0.64 in the CorpAppliance group. It uses HTTP protocol on port 8014 with an encrypted password or preshared secret of symantec.

3   Check the communication status of Enforcer appliance and the Symantec Endpoint Protection Manager.

    See "Checking the communication status of an Enforcer appliance on the Enforcer console" on page 854.

4   Configure, deploy, and install or download client software if you have not already done so.

    To allow guests (unmanaged client computers) to automatically download Symantec Network Access Control On-Demand Clients, configure a Gateway Enforcer to manage the automatic downloading process.

    See "Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network" on page 1054.

configure spm

The configure SPM command sets up the connection between the Enforcer appliance and the Symantec Endpoint Protection Manager.

You must type all values if you change any of the values. Any values that you do not specify automatically use default values.

The configure spm command uses the following syntax:

```
configure spm {[ip <ipaddress>] | [group
<group-name>] | [http <port-number>] | https
<port-number>] | [key <key-name>]} | [del key
<shared-key>]
```

where:

ip <ipaddress>	Enables you to add the IP address of the Symantec Endpoint Protection Manager.
del key <shared-key>	Delete shared secret key.
group <group-name>	Enables you to specify a preferred group name for the Enforcer appliance. Therefore it is recommended that you assign a unique group name to distinguish the Enforcer appliances on the console of the Symantec Endpoint Protection Manager.
http <port-number>	Enables you to specify the HTTP protocol and the port number to communicate with the Symantec Endpoint Protection Manager. The default protocol is HTTP. The default port number for the HTTP protocol is 80.
https <port-number>	Enables you to specify the HTTPS protocol and the port number to communicate with the Symantec Endpoint Protection Manager. You should only use this command if the Symantec Endpoint Protection Manager has been set up to use the HTTPS protocol. The default port number for the HTTPS protocol is 443.
key <key-name>	Enables you to specify the encrypted password that is required if the Symantec Endpoint Protection Manager has been installed with one.

The following example describes configuring an Enforcer appliance to communicate with the Symantec Endpoint Protection Manager at IP address 192.168.0.64 in an Enforcer group called CorpAppliance. It uses the HTTP protocol on port 80 with an encrypted password of "security."

```
configure spm ip 192.168.0.64 group CorpAppliance http 80 key security
```

Checking the communication status of an Enforcer appliance on the Enforcer console

You can check the communication status of an Enforcer appliance from the Enforcer console.

To check the communication status of an Enforcer appliance on the Enforcer console

1   Log on to the Enforcer console if you are not already logged on.

See "Logging on to an Enforcer appliance" on page 804.

2   Type the following command: **show status**

You can view information about the current connection status.

The following example indicates that the Enforcer appliance is online and connected to a Symantec Endpoint Protection Manager with an IP address of 192.168.0.1 and communication port 8014:

```
Enforcer#: show status
Enforcer Status:        ONLINE(ACTIVE)
Policy Manager Connected: YES
Policy Manager:         192.168.0.1 HTTP 8014
Packets Received:       3659
Packets Transmitted:    3615
Packet Receive Failed:  0
Packet Transfer Failed: 0
Enforcer Health:        EXCELLENT
Enforcer Uptime:        10 days 01:10:55
Policy ID:              24/03/2010  21:31:55
```

Remote access to an Enforcer appliance

To securely communicate with the Enforcer for command-line access, use one of the following methods:

■ Networked KVM switch or similar device

■ SSH client which supports SSH v2 Terminal Console server

■ Serial cable

See "Setting up an Enforcer appliance" on page 803.

About the Enforcer appliance CLI command hierarchy

The Enforcer appliance uses a command-line interface (CLI) that is organized into the following groups:

■ capture

■ configure

- console

- debug

- mab

- monitor

- on-demand

- snmp

For a complete listing of the command-line interface command groups and commands, see the *Symantec Network Access Control Enforcer Command-line Reference Guide*, located at:

http://www.symantec.com/business/support/
documentation.jsp?language=english&view=manuals&pid=52788

Planning for the installation of the Gateway Enforcer appliance

This chapter includes the following topics:

- Installation planning for a Gateway Enforcer appliance
- Gateway Enforcer appliance NIC settings
- Failover planning for Gateway Enforcer appliances
- Fail-open and fail-closed planning for a Gateway Enforcer appliance

Installation planning for a Gateway Enforcer appliance

A Gateway Enforcer appliance is generally used inline as a secure policy-enforcing bridge to protect a corporate network from external intruders. Before you install a Gateway Enforcer appliance, you need to think about locating it appropriately on the network. Gateway Enforcer appliances can be placed throughout the enterprise to ensure that all endpoints comply with the security policy.

Another use of the Gateway Enforcer appliance is hosting on-demand clients for guest-users. These clients are provided with temporary access to the Enforcer, have their security credentials verified, and are then permitted onto the network.

See "About the Symantec Network Access Control On-Demand Clients" on page 1048.

The Gateway Enforcer in this case is not passing packets through, but rather serving as a host. This capability is not often used, and is thus done from the command line of the Enforcer.

```
configure > advanced > guest-enf enable
```

See "About the Enforcer appliance CLI command hierarchy" on page 855.

Note: If you are upgrading from Symantec Sygate Endpoint Protection 5.1 clients, you must upgrade Symantec Endpoint Protection Manager first, then your Enforcers, then your clients, moving them to version 12.1 first. Once you have Symantec Endpoint Protection Manager and your Enforcers at version 11.x, you must check **Allow Legacy Clients** on the Enforcer menu, if you have clients older than 11.x, before you take the final step. Then finish the upgrade to the current release.

Gateway Enforcer appliances typically are in use in the following network locations:

- VPN
- Wireless access point (WAP)
- Dial-up (Remote access server [RAS])
- Ethernet (local area network [LAN]) segments

Several types of planning information can help you implement Gateway Enforcer appliances in a network.

General placement:

- See "Where to place a Gateway Enforcer appliance" on page 859.
- See "Guidelines for IP addresses on a Gateway Enforcer appliance" on page 861.
- See "About two Gateway Enforcer appliances in a series" on page 861.

Specific areas of the network:

- See "Protection of VPN access through a Gateway Enforcer appliance" on page 862.
- See "Protection of wireless access points through a Gateway Enforcer appliance" on page 862.
- See "Protection of servers through a Gateway Enforcer appliance" on page 862.
- See "Protection of non-Windows servers and clients through a Gateway Enforcer appliance" on page 863.
- See "Requirements for allowing non-Windows clients without authentication" on page 864.

Where to place a Gateway Enforcer appliance

You can place Gateway Enforcers at locations where all traffic must pass through a Gateway Enforcer before a client can do the following actions:

■ Connect to a corporate network.

■ Reach the secured areas of a network.

See "Guidelines for IP addresses on a Gateway Enforcer appliance" on page 861.

You typically can place Gateway Enforcer appliances at the following locations:

VPN	Between virtual private network (VPN) concentrators and the corporate network
Wireless Access Point (WAP)	Between a wireless access point and the corporate network
Servers	In front of corporate servers

Larger organizations may require a Gateway Enforcer appliance to protect every network entry point. Gateway Enforcers are typically located in different subnets. In most cases, you can integrate Gateway Enforcer appliances into a corporate network without having to make hardware configuration changes.

Gateway Enforcer appliances must use two network interface cards (NICs).

Figure 46-1 shows how to place Gateway Enforcer appliances in the overall network configuration.

Figure 46-1   Placement of Gateway Enforcer appliances
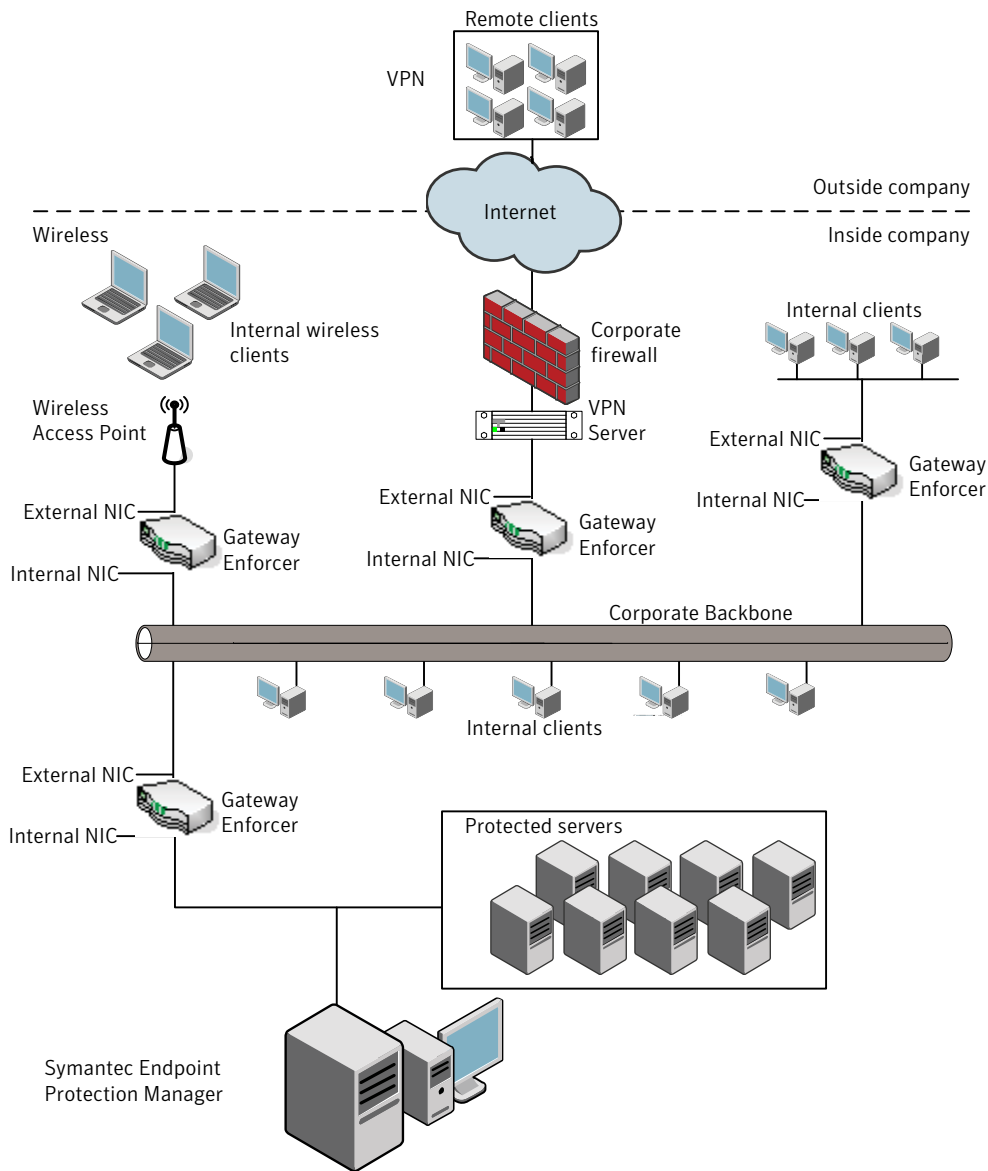
Another location where a Gateway Enforcer appliance protects a network is at a Remote Access Server (RAS). Clients can dial up to connect to a corporate network. RAS dial-up clients are configured similarly to wireless and VPN clients. The

external NIC connects to the RAS server and the internal NIC connects to the network.

Guidelines for IP addresses on a Gateway Enforcer appliance

Follow these guidelines when you set up the internal NIC address for a Gateway Enforcer appliance:

- A Gateway Enforcer appliance's internal NIC must be able to communicate with a Symantec Endpoint Protection Manager. By default, the internal NIC must face a Symantec Endpoint Protection Manager.

- Clients must be able to communicate with the Gateway Enforcer appliance's internal IP address. The VPN server or wireless AP can be in a different subnet. This works if the clients can be routed to the same subnet as the Gateway Enforcer appliance's internal IP address.

- For the Gateway Enforcer appliance that protects internal servers, the internal NIC connects to the VLAN that in turn connects to the servers.

- If you use multiple Gateway Enforcer appliances in a failover configuration, the IP address of the internal NIC on each Gateway Enforcer appliance must have its own IP address.

The Gateway Enforcer generates a bogus external NIC address, based on the internal NIC address. You do not need to configure this address again if you install another Gateway Enforcer.

See "Setting up an Enforcer appliance" on page 803.

About two Gateway Enforcer appliances in a series

If a network supports two Gateway Enforcer appliances in a series so that a client connects to the network through more than one Gateway Enforcer appliance, you must specify the Enforcer appliance that is closest to the Symantec Endpoint Protection Manager as a trusted internal IP address of the other Gateway Enforcer appliance. Otherwise a 5-minute delay can occur before the client can connect to the network.

This delay can occur when the client runs a Host Integrity check that fails. As part of Host Integrity remediation, the client downloads the required software updates. Then the client runs the Host Integrity check again. At that point the Host Integrity check passes, but network access is delayed.

See "Adding a trusted internal IP address for clients on a management server" on page 898.

Protection of VPN access through a Gateway Enforcer appliance

The protection of VPN access is the first and the most common reason to use a Gateway Enforcer appliance. You can place Gateway Enforcer appliances at VPN entry points to secure access to a corporate network. The Gateway Enforcer appliance is placed between the VPN server and the corporate network. It allows access only to authorized users and prevents access by anyone else.

See "Where to place a Gateway Enforcer appliance" on page 859.

See "Setting up an Enforcer appliance" on page 803.

Protection of wireless access points through a Gateway Enforcer appliance

Enforcer appliances protect the corporate network at wireless access points (WAP). The Gateway Enforcer appliance ensures that anyone who connects to the network by using wireless technology runs the client and meets the security requirements.

After these conditions are met, the client is granted access to the network. The Gateway Enforcer appliance is placed between the WAP and the corporate network. The external NIC points toward the WAP and the internal NIC points toward the corporate network.

See "Where to place a Gateway Enforcer appliance" on page 859.

See "Setting up an Enforcer appliance" on page 803.

Protection of servers through a Gateway Enforcer appliance

Gateway Enforcer appliances can protect the corporate servers that hold sensitive information in the corporate network. An organization may place important data on the servers that may be located in a locked computer room. Only system administrators may have access to the locked computer room.

The Gateway Enforcer appliance acts like an additional lock on the door. It does so by allowing only the users that meet its criteria to access the protected servers. Servers locate the internal NIC in this setup. However, users who try to gain access must pass through the external NIC.

To safeguard these servers, you can limit access only to clients with designated IP addresses and you can set up strict Host Integrity rules. For example, you can configure a Gateway Enforcer appliance to protect servers in a network. A Gateway Enforcer appliance can be located between clients on a corporate LAN and the servers that it safeguards. The external NIC points to the corporate LAN inside the company and the internal NIC points toward the protected servers. This

configuration prevents unauthorized users or clients from gaining access to the servers.

See "Where to place a Gateway Enforcer appliance" on page 859.

See "Setting up an Enforcer appliance" on page 803.

Protection of non-Windows servers and clients through a Gateway Enforcer appliance

You can install the servers and the clients on an operating system other than Microsoft Windows. However, the Gateway Enforcer appliance cannot authenticate any servers and clients that do not run on a computer that does not support Microsoft Windows.

If an organization includes servers and clients with operating systems on which the client software is not installed, you must decide which of the following methods to use:

- Implement support through a Gateway Enforcer appliance.

- See "Implementation of non-Windows support through a Gateway Enforcer appliance" on page 863.

- Implement support without a Gateway Enforcer appliance.
  See "Implementation of support for non-Windows clients without a Gateway Enforcer appliance" on page 863.

Implementation of non-Windows support through a Gateway Enforcer appliance

You can implement support for non-Windows clients by configuring the Gateway Enforcer appliance to allow all non-Windows clients to access the network. If you configure the Gateway Enforcer appliance in this way, it performs operating system detection to identify the clients that run non-Windows operating systems.

See "Where to place a Gateway Enforcer appliance" on page 859.

See "Setting up an Enforcer appliance" on page 803.

Implementation of support for non-Windows clients without a Gateway Enforcer appliance

You can implement support for non-Windows clients by allowing non-Windows clients to access the network through a separate access point.

You can connect the following clients that support non-Windows operating systems through a separate VPN server:

- One VPN Server can support the clients that have the client software installed on them. The Windows-based client computers can connect to the corporate network through a Gateway Enforcer appliance.

- Another VPN server can support the clients that run non-Windows operating systems. The non-Windows-based client computer can then connect to the corporate network without a Gateway Enforcer appliance.

See "Where to place a Gateway Enforcer appliance" on page 859.

See "Setting up an Enforcer appliance" on page 803.

Requirements for allowing non-Windows clients without authentication

You can configure the Gateway Enforcer appliance to allow non-Windows clients without authentication.

See "Requirements for non-Windows clients" on page 865.

When a client tries to access the network through a Gateway Enforcer appliance, the Enforcer appliance first checks whether the client software has been installed on the client computer. If the client software is not running and if the option to allow non-Windows clients is set, the Gateway Enforcer appliance checks the operating system.

It checks the operating system by sending packets of information to probe the client to detect the type of operating system that it currently runs. If the client runs a non-Windows operating system, the client is allowed regular network access.

Requirements for Windows clients

When a Gateway Enforcer appliance is configured to allow non-Windows clients to connect to a network, it first tries to determine a client's operating system. If the operating system is a Windows-based operating system, the Gateway Enforcer appliance authenticates the client. Otherwise, the Gateway Enforcer appliance allows the client to connect to the network without authentication.

The Gateway Enforcer appliance correctly detects the Windows operating system if the Windows client meets the following requirements:

- The Client for Microsoft Networks option must be installed and enabled on the client.
  See the Windows documentation.

- The UDP port 137 must be open on the client. It must be accessible by the Gateway Enforcer.

If a Windows client fails to meet these requirements, the Gateway Enforcer appliance may interpret the Windows client to be a non-Windows client. Therefore the Gateway Enforcer appliance can allow the non-Windows client to connect to the network without authentication.

See "Allowing non-Windows clients to connect to a network without authentication" on page 887.

Requirements for non-Windows clients

The Gateway Enforcer appliance must meet the following requirements before it allows a Mac client to connect to a network:

- Windows Sharing must be on.
  This default setting is enabled.

- Mac built-in firewall must be off.
  This setting is the default.

The Gateway Enforcer has the following requirement to allow a Linux client:

- The Linux system must run the Samba service.

See "Allowing non-Windows clients to connect to a network without authentication" on page 887.

Gateway Enforcer appliance NIC settings

The network interface cards (NICs) on a Gateway Enforcer appliance are configured by default so that eth0 is used for the internal NIC. The internal NIC must connect to the Symantec Endpoint Protection Manager.

You can use the configure interface-role command if you need to change which NIC is external and which is internal.

Note: If you use the Gateway Enforcer to download On-Demand clients and you have enabled 801.Q trunking on the switch, check the NIC connection speed. To successfully download the On-Demand client, both NICs must connect to the switch with the same connection speed.

See "About the Enforcer appliance CLI command hierarchy" on page 855.

Failover planning for Gateway Enforcer appliances

An enterprise can support two Gateway Enforcer appliances that are configured to continue operations when one of the Gateway Enforcer appliances fails. If a Gateway Enforcer appliance fails in a network that is not configured for failover, then network access at that location is automatically blocked. If a Gateway Enforcer appliance fails in a network that does not provide for failover, the clients can no longer connect to the network. The clients continue to be blocked from connecting to the network until the problem with the Gateway Enforcer appliance is corrected.

For a Gateway Enforcer appliance, failover is implemented through the Gateway Enforcer appliance itself instead of third-party switches. If the configuration is set up correctly, the Symantec Endpoint Protection Manager automatically synchronizes the settings for the failover Gateway Enforcer appliances.

Note: Failover capabilities are not possible if your Enforcers are set in fail-open mode. Choose to have failover capabilities or fail-open. The choices are mutually exclusive.

See "Setting up Gateway Enforcer appliances for failover" on page 869.

See "Fail-open and fail-closed planning for a Gateway Enforcer appliance" on page 869.

How failover works with Gateway Enforcer appliances in the network

The Gateway Enforcer appliance that is operational is called the active Gateway Enforcer appliance. The backup Gateway Enforcer appliance is called the standby Gateway Enforcer appliance. The active Gateway Enforcer appliance is also referred to as the primary Gateway Enforcer appliance. If the active Gateway Enforcer appliance fails, the standby Gateway Enforcer appliance takes over the enforcement tasks.

The sequence in which the two Gateway Enforcer appliances are started is as follows:

- When the first Gateway Enforcer appliance is started, it runs in standby mode. While in standby mode, it queries the network to determine whether another Gateway Enforcer appliance runs. It sends out three queries to search for another Gateway Enforcer. Therefore it can take a few minutes to change its status to Online.

- If the first Gateway Enforcer appliance does not detect another Gateway Enforcer appliance, the first Gateway Enforcer appliance becomes the active Gateway Enforcer appliance.

- While the active Gateway Enforcer appliance runs, it broadcasts failover packets on both the internal and the external networks. It continues to broadcast the failover packets.

- As soon as the second Gateway Enforcer appliance is started, it runs in standby mode. It queries the network to determine whether another Gateway Enforcer appliance runs.

- The second Gateway Enforcer appliance then detects the active Gateway Enforcer appliance that is running and therefore remains in standby mode.

- If the active Gateway Enforcer appliance fails, it stops to broadcast failover packets. The standby Gateway Enforcer appliance no longer detects an active Gateway Enforcer appliance. Therefore it now becomes the active Gateway Enforcer appliance that handles network connections and security at this location.

- If you start the other Gateway Enforcer appliance, it remains the standby Gateway Enforcer appliance because it detects that another Gateway Enforcer appliance is active.

See "Setting up Gateway Enforcer appliances for failover" on page 869.

Where to place Gateway Enforcer appliances for failover in a network with one or more VLANs

You set up a Gateway Enforcer appliance for failover by its physical location and by the configuration that you perform on the Symantec Endpoint Protection Manager. If you use a hub that supports multiple VLANs, you can use only one VLAN unless you integrate an 802.1Q-aware switch instead of a hub.

The Gateway Enforcer appliance for failover must be set up on the same network segment. A router or gateway cannot be installed between the two Gateway Enforcer appliances. A router or gateway does not forward the failover packet. The internal NICs must both connect to the internal network through the same switch or hub. The external NICs must both connect to the external VPN server or access point through the same switch or hub.

You use similar processes to configure Gateway Enforcer appliances for failover at a wireless AP, dial-up RAS, or other access points. The external NICs of both Gateway Enforcer appliances connect to the external network through a wireless AP or RAS server. The internal NICs connect to the internal network or area that is protected.

Figure 46-2 shows how to set up two Gateway Enforcer appliances for failover to protect network access at a VPN concentrator.

Figure 46-2   Placement of two Gateway Enforcer appliances
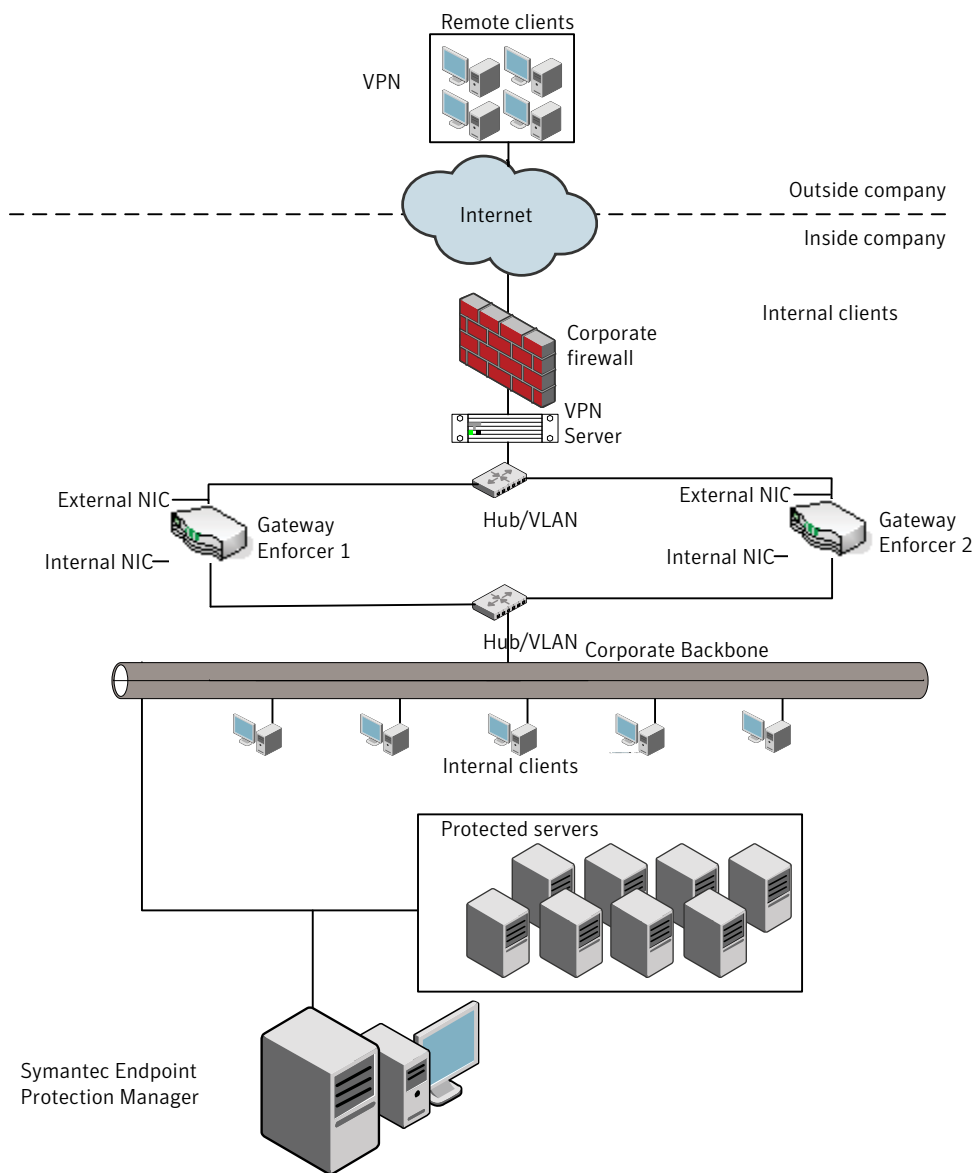
Setting up Gateway Enforcer appliances for failover

You should familiarize yourself with the concepts that are involved in Gateway Enforcer appliance failover before you set up standby Enforcers.

See "How failover works with Gateway Enforcer appliances in the network" on page 866.

To set up Gateway Enforcer appliances for failover

1   Place the computers in the network.

    See "Where to place Gateway Enforcer appliances for failover in a network with one or more VLANs" on page 867.

2   Set up the internal NICs.

    The internal NICs on multiple Gateway Enforcer appliances must each have a different IP address.

    See "Guidelines for IP addresses on a Gateway Enforcer appliance" on page 861.

Fail-open and fail-closed planning for a Gateway Enforcer appliance

Fail-open is available for Gateway Enforcer appliance models with a fail-open NIC. Fail-open is an alternative to failover that provides network availability when the Enforcer service is not available.

Note: Beginning with Symantec Network Access Control version 11.0 RU6 MP1, Enforcers will ship with a Silcom NIC card that is in configured in fail-open mode. To configure the Enforcer to be in fail-closed mode, issue the following CLI command:

```
configure interface failopen disable
```

Note: Failover capabilities are not possible if your Enforcers are set in fail-open mode. Choose to have failover capabilities or fail-open. The choices are mutually exclusive.

See "Installing an Enforcer appliance" on page 800.

See "Failover planning for Gateway Enforcer appliances" on page 866.

Configuring the Symantec Gateway Enforcer appliance from the Symantec Endpoint Protection Manager

This chapter includes the following topics:

■ About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console

■ Changing Gateway Enforcer appliance configuration settings in Symantec Endpoint Protection Manager

■ About general settings on a Gateway appliance

■ About authentication settings on a Gateway appliance

■ Authentication range settings

■ About advanced Gateway Enforcer appliance settings

About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console

You can add or edit the configuration settings for the Gateway Enforcer appliance in the Symantec Endpoint Protection Manager Console.

Before you can proceed, you must complete the following tasks:

■ Install the software for the Symantec Endpoint Protection Manager on a computer.
   See "Installing Symantec Endpoint Protection Manager" on page 95.
   The computer on which the Symantec Endpoint Protection Manager software is installed is also referred to as the management server.

■ Connect the Symantec Gateway Enforcer appliance to the network.
   See "Setting up an Enforcer appliance" on page 803.

■ Configure the Symantec Gateway Enforcer appliance on the local Gateway Enforcer console during the installation.
   See "Configuring an Enforcer appliance" on page 805.

After you finish these tasks, you can specify additional configuration settings for the Gateway Enforcer appliance on a management server.

When you install a Gateway Enforcer appliance, a number of default settings and ports are automatically set up. The default settings for the Gateway Enforcer appliance on the Symantec Endpoint Protection Manager allow all clients to connect to the network if the client passes the Host Integrity check. The Gateway Enforcer appliance acts as a bridge. Therefore you can complete the process of setting up the Gateway Enforcer appliance and deploying clients without blocking access to the network.

However, you need to change the default settings on Symantec Endpoint Protection Manager to limit which clients are allowed access without authentication. Optionally, there are other Enforcer default settings for the Gateway Enforcer appliance that you may want to customize before you start enforcement.

Changing Gateway Enforcer appliance configuration settings in Symantec Endpoint Protection Manager

You can change the Gateway Enforcer appliance configuration settings on a management server. The configuration settings are automatically downloaded

from the management server to the Gateway Enforcer appliance during the next heartbeat.

To change Gateway Enforcer appliance configuration settings in Symantec Endpoint Protection Manager

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   In the **Admin** page, click **Servers**.

3   In **Servers**, select the group of Enforcers of which the Gateway Enforcer appliance is a member.

    The Enforcer group must include the Gateway Enforcer appliance for which the configuration settings must be changed.

4   Select the Gateway Enforcer appliance for which the configuration settings must be changed.

5 Under **Tasks**, click **Edit Group Properties**.

6 In the **Settings** dialog box, change any of the configuration settings.

The **Gateway Enforcer Settings** dialog box provides the following categories of configuration settings:

General	Settings for the Enforcer group description and management server list.
	See "About general settings on a Gateway appliance" on page 875.
Authentication	Settings for a variety of parameters that affect the client authentication process.
	If a matching address is still not found, the Gateway Enforcer appliance begins the authentication session and sends the challenge packet.
	See "About authentication settings on a Gateway appliance" on page 878.
Auth Range	Settings that specify an individual IP address for a client or IP address ranges for clients who need to be authenticated. You can also specify an individual IP address or IP address ranges for the clients that are allowed to connect to a network without authentication.
	See "Authentication range settings" on page 892.
Advanced	Settings for authentication timeout parameters and Gateway Enforcer appliance message timeouts.
	Settings for MAC addresses for the trusted hosts that the Gateway Enforcer appliance allows to connect without authentication (optional).
	Settings for DNS Spoofing and Local Authentication.
	Settings for protocols to be allowed without blocking clients.
	See "About advanced Gateway Enforcer appliance settings" on page 902.
Log Settings	Settings for enabling logging of Server logs, Client Activity logs, and specifying log file parameters.
	See "About Enforcer reports and logs" on page 976.
	See "Configuring Enforcer log settings" on page 977.

About general settings on a Gateway appliance

You can add or edit the description of a Gateway Enforcer appliance or a Gateway Enforcer appliance group in Symantec Endpoint Protection Manager.

See "Adding or editing the description of a Gateway Enforcer appliance group" on page 875.

See "Adding or editing the description of a Gateway Enforcer appliance" on page 876.

You cannot add or edit the name of a Gateway Enforcer appliance group in the Symantec Endpoint Protection Manager. You cannot add or edit the IP address or host name of a Gateway Enforcer appliance in the Symantec Endpoint Protection Manager. Instead, you must perform these tasks on the Enforcer console.

You can add or edit the IP address or host name of a Gateway Enforcer appliance in a management server list.

See "Adding or editing the IP address or host name of a Gateway Enforcer appliance" on page 876.

You can also add or edit the IP address or host name of a Symantec Endpoint Protection Manager in a management server list.

See "Establishing communication between a Gateway Enforcer appliance and a Symantec Endpoint Protection Manager through a management server list and the conf.properties file" on page 877.

Adding or editing the description of a Gateway Enforcer appliance group

You can add or edit the description of an Enforcer group of which a Symantec Gateway Enforcer appliance is a member. You can perform this task on the Symantec Endpoint Protection Manager console instead of the Enforcer console.

See "About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console" on page 872.

See "About general settings on a Gateway appliance" on page 875.

To add or edit the description of a Gateway Enforcer appliance group

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the Gateway Enforcer appliance group whose description you want to add or edit.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Settings** dialog box, on the **General** tab, add or edit a description for the Gateway Enforcer appliance group in the **Description** field.

6   Click **OK**.

Adding or editing the description of a Gateway Enforcer appliance

You can add or edit the description of a Gateway Enforcer appliance. You can perform this task on the Symantec Endpoint Protection Manager console instead of the Enforcer console. After you complete this task, the description appears in Description field of the Management Server pane.

See "About general settings on a Gateway appliance" on page 875.

See "About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console" on page 872.

To add or edit the description of a Gateway Enforcer appliance

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the Gateway Enforcer appliance group whose description you want to add or edit.

4   Select the Gateway Enforcer appliance whose description you want to add or edit.

5   Under **Tasks**, click **Edit Enforcer Properties**.

6   In the **Enforcer Properties** dialog box, add or edit a description for the Gateway Enforcer appliance in the Description field.

7   Click **OK**.

Adding or editing the IP address or host name of a Gateway Enforcer appliance

You can change the IP address or host name of a Gateway Enforcer appliance on the Gateway Enforcer console only during the installation. If you want to change the IP address or host name of a Gateway Enforcer appliance at a later time, you can do so on a Gateway Enforcer console.

See "About the Enforcer appliance CLI command hierarchy" on page 855.

See "About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console" on page 872.

See "About general settings on a Gateway appliance" on page 875.

Establishing communication between a Gateway Enforcer appliance and a Symantec Endpoint Protection Manager through a management server list and the conf.properties file

Gateway Enforcer appliances must be able to connect to servers on which the Symantec Endpoint Protection Manager is installed. The Symantec Endpoint Protection Manager includes a file that helps manage the traffic between clients, management servers, and optional Enforcers such as a Gateway Enforcer appliance.

This file is called a management server list. The management server list specifies to which Symantec Endpoint Protection Manager a Gateway Enforcer connects. It also specifies to which Symantec Endpoint Protection a Gateway Enforcer connects in case of a management server's failure.

A default management server list is automatically created for each site during the initial installation. All available management servers at that site are automatically added to the default management server list.

A default management server list includes the management server's IP addresses or host names to which Gateway Enforcer appliances can connect after the initial installation. You may want to create a custom management server list before you deploy any Gateway Enforcer appliances. If you create a custom management server list, you can specify the priority in which a Gateway Enforcer appliance can connect to management servers.

If an administrator has created multiple management server lists, you can select the specific management server list that includes the IP addresses or host names of those management servers to which you want the Gateway Enforcer appliance to connect. If there is only one management server at a site, then you can select the default management server list. You can also select the management server list that you want an Enforcer group to be able to roam among, making choices in the same dialog box.

See "Configuring a management server list" on page 740.

See "About configuring the Symantec Gateway Enforcer appliance on the Symantec Endpoint Protection Manager Console" on page 872.

See "About general settings on a Gateway appliance" on page 875.

To establish communication between a Gateway Enforcer between a Symantec Endpoint Protection Manager

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3 Select and expand the group of Enforcers.

The Enforcer group must include the Gateway Enforcer appliance for which you want to change the IP address or host name in a management server list.

4 Under **Tasks**, click **Edit Group Properties**.

5 In the **Settings** dialog box, on the **General** tab, under **Communication**, select the management server list that you want this Gateway Enforcer appliance to use.

6 Click **Select**.

You can view the IP addresses and host names of all available management servers, as well as the priorities that have been assigned to them.

7 In the **Management Server List** dialog box, click **Close**.

8 In the **Settings** dialog box, click **OK**.

You can also turn on and off whether the Management Server is listening for the Enforcer, by changing a line in the `conf.properties` file.

To configure the Management Server to listen for the Enforcer thread by editing the `conf.properties` file

1 Open the `conf.properties` file in a simple text editor such as Notepad.

The `conf.properties` file is located in the following folder: `C:\Program Files\Symantec\Symantec Endpoint Protection Manager\tomcat\etc`.

2 Find the line that begins with `scm.radius.port.enabled`

3 To disable the Enforcer thread, append `=0` to the line, resulting in `scm.radius.port.enabled=0`

4 To enable the Enforcer thread, append `=1` to the line, resulting in `scm.radius.port.enabled=1`

About authentication settings on a Gateway appliance

You can specify a number of authentication settings for a Gateway Enforcer appliance authentication session. When you apply these changes, they are automatically sent to the selected Gateway Enforcer appliance during the next heartbeat.

See "Authentication settings on a Gateway appliance" on page 879.

Authentication settings on a Gateway appliance

You may want to implement a number of authentication settings to further secure the network.

Table 47-1 provides more information about the options on the **Authentication** tab.

Table 47-1   Authentication configuration settings for a Gateway Enforcer appliance

Option	Description
Maximum number of packets per authentication session	The maximum number of challenge packets that the Gateway Enforcer appliance sends in each authentication session. The default number is 10 packets. The range is 2 through 100 packets. See "Specifying the maximum number of challenge packets during an authentication session" on page 883.
Time between packets in authentication session (seconds)	The time in seconds between each challenge packet that the Enforcer sends. The default value is 3 seconds. The range is 3 through 10. See "Specifying the frequency of challenge packets to be sent to clients" on page 884.
Time rejected client will be blocked (seconds)	The amount of time in seconds for which a client is blocked after it fails authentication. The default setting is 30 seconds. The range is 10 through 300 seconds. See "Specifying the time period for which a client is blocked after it fails authentication" on page 885.
Time authenticated client will be allowed (seconds)	The amount of time in seconds for which a client is allowed to retain its network connection without reauthentication. The default setting is 30 seconds. The range is 10 through 300 seconds. See "Specifying the time period for which a client is allowed to retain its network connection without reauthentication" on page 886.

Table 47-1 Authentication configuration settings for a Gateway Enforcer appliance *(continued)*

Option	Description
Allow all clients, but continue to log which clients are not authenticated	If this option is enabled, the Gateway Enforcer appliance authenticates all users by checking that they are running a client. The Gateway Enforcer appliance also checks if the client passed the Host Integrity check. If the client passes the Host Integrity check, the Gateway Enforcer appliance then logs the results. It then forwards the Gateway request to receive a normal rather than a quarantine network configuration, whether the checks pass or fail. The default setting is not enabled. See "Allowing all clients with continued logging of non-authenticated clients" on page 886.
Allow all clients with non-Windows operating systems	If this option is enabled, the Gateway Enforcer checks for the operating system of the client. The Gateway Enforcer appliance then allows all clients that do not run the Windows operating systems to receive a normal network configuration without being authenticated. If this option is not enabled, the clients receive a quarantine network configuration. The default setting is not enabled. See "Allowing non-Windows clients to connect to a network without authentication" on page 887.
Check the Policy Serial Number on Client before allowing Client into network	If this option is enabled, the Gateway Enforcer appliance verifies that the client has received the latest security policies from the management server. If the policy serial number is not the latest, the Gateway Enforcer notifies the client to update its security policy. The client then forwards the Gateway request to receive a quarantine network configuration. If this option is not enabled and if the Host Integrity check succeeds, the Gateway Enforcer appliance forwards the Gateway request to receive a normal network configuration. The Gateway Enforcer forwards the request even if the client does not have the latest security policy. The default setting is not enabled. See "Checking the policy serial number on a client" on page 888.

Table 47-1   Authentication configuration settings for a Gateway Enforcer
appliance *(continued)*

Option	Description
Enable pop-up message on client if Client is not running	If this option is enabled, a message appears to users on Windows computers that try to connect to an enterprise network without running a client. The default message is set to display only one time. The message tells the users that they are blocked from accessing the network because a client is not running and tells them to install it. To edit the message or to change how often it is displayed, you can click Message. The maximum message length is 128 characters.
	The default setting is enabled.
	Note: Popup messages do not appear on Mac clients.
	See "Sending a message from a Gateway Enforcer appliance to a client about non-compliance" on page 889.
Enable HTTP redirect on client if Client is not running	If this option is enabled, the Gateway Enforcer can redirect clients to a remediation Web site.
	If this option is enabled, the Gateway Enforcer appliance redirects HTTP requests to an internal Web server if the client does not run.
	This option cannot be enabled without having specified a URL.
	The default setting is enabled, with the value http://localhost.
	See "Redirecting HTTP requests to a Web page" on page 891.
HTTP redirect URL	You can specify a URL of up to 255 characters when you redirect clients to a remediation Web site.
	The default setting for the redirect URL is http://localhost.
	See "Redirecting HTTP requests to a Web page" on page 891.
HTTP redirect port	You can specify a port number other than 80 when you redirect clients to a remediation Web site.
	The default setting for the Web server is port 80.
	See "Redirecting HTTP requests to a Web page" on page 891.

About authentication sessions on a Gateway Enforcer appliance

When a client tries to access the internal network, the Gateway Enforcer establishes an authentication session with it. An authentication session is a set of challenge packets that are sent from a Gateway Enforcer appliance to a client.

During an authentication session, the Gateway Enforcer appliance sends a challenge packet to the client at a specified frequency. The default setting is every three seconds. It keeps sending packets until it receives a response from the client, or until it has sent out the maximum number of packets specified. The default number is 10 packages.

If the client responds and passes authentication, the Gateway Enforcer appliance allows it access to the internal network for a specified number of seconds. The default is 30 seconds. The Gateway Enforcer appliance starts a new authentication session during which the client must respond to retain the connection to the internal network. The Gateway Enforcer appliance disconnects the clients that do not respond or are rejected because they fail authentication.

If the client does not respond or fails authentication, the Gateway Enforcer appliance blocks it for a specified number of seconds. The default is 30 seconds. If another client tries to log on using that same IP address, it has to be reauthenticated.

You can configure the authentication session for each Gateway Enforcer appliance on the management server.

See "Changing Gateway Enforcer appliance configuration settings in Symantec Endpoint Protection Manager" on page 872.

See "Authentication settings on a Gateway appliance" on page 879.

About client authentication on a Gateway Enforcer appliance

The Gateway Enforcer appliance authenticates remote clients before it allows access to the network. Client authentication in the Gateway Enforcer performs the following functions:

- Determines whether to authenticate the client or allow it without authentication
  You can specify individual clients or ranges of IP addresses to trust or to authenticate on the **Auth Range** tab.

- Carries out the authentication session
  You configure the settings for the authentication session on the **Authentication** tab.

Each Gateway Enforcer maintains the following lists of trusted IP addresses that are allowed to connect to the network through the Gateway Enforcer:

- A static list
  The trusted external IP addresses that are configured for the Enforcer on the **Auth Range** tab.

- A dynamic list
  The additional trusted IP addresses that are added and dropped as clients are authenticated, allowed to connect to the network, and finally disconnected.

When traffic arrives from a new client, the Gateway Enforcer appliance determines whether this client is included in the list of trusted client IP addresses. If the client has a trusted IP address, it is allowed on the network with no further authentication.

If the client lacks a trusted IP address, the Gateway Enforcer appliance checks if the trusted IP address is within the client IP address range for the clients that should be authenticated. If the client's IP address is within the client IP address range, the Gateway Enforcer appliance begins an authentication session.

During the authentication session, the client sends its unique ID number, the results of the Host Integrity check, and its policy serial number. The policy serial number identifies if the client security policies are up to date.

The Gateway Enforcer appliance checks the results. It can optionally check the policy serial number. If the results are valid, the Gateway Enforcer appliance gives the client an authenticated status and allows network access to the client. If the results are not valid, the Gateway Enforcer appliance blocks the client from connecting to the network.

When a client is authenticated, that client's IP address is added to the dynamic list with a timer. The default timer interval is 30 seconds. After the timer interval has elapsed, the Gateway Enforcer appliance begins a new authentication session with the client. If the client does not respond or fails authentication, the client's IP address is deleted from the list. The IP address is also blocked for a specified interval. The default setting is 30 seconds. When another client tries to log on by using that same IP address, the client has to be reauthenticated.

See "Authentication settings on a Gateway appliance" on page 879.

Specifying the maximum number of challenge packets during an authentication session

During the authentication session, the Gateway Enforcer appliance sends a challenge packet to the client at a specified frequency.

The Gateway Enforcer appliance continues to send packets until the following conditions are met:

- The Gateway Enforcer appliance receives a response from the client.

- The Gateway Enforcer appliance has sent the specified maximum number of packets.

The default setting is 10 packets for the maximum number of challenge packets for an authentication session. The range is from 2 through 100 packets.

See "About authentication settings on a Gateway appliance" on page 878.

To specify the maximum number of challenge packets during an authentication session

1   In Symantec Endpoint Protection Manager, click **Admin**.

2   Click **Servers**.

3   Select and expand the group of Enforcers.

    The Enforcer group must include the Gateway Enforcer appliance for which you want to specify the maximum number of challenge packets during an authentication session.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Gateway Settings** dialog box, on the **Authentication** tab, under **Authentication Parameters** type the maximum number of challenge packets that you want to allow during an authentication session in the **Maximum number of packets per authentication session** field.

    The default setting is 10 seconds. The range is from 2 through 100 packets.

6   Click **OK**.

Specifying the frequency of challenge packets to be sent to clients

During the authentication session, the Gateway Enforcer appliance sends a challenge packet to the client at a specified frequency.

The Gateway Enforcer appliance continues to send packets until the following conditions are met:

- The Gateway Enforcer appliance receives a response from the client.

- The Gateway Enforcer appliance has sent the specified maximum number of packets.

The default setting is every 3 seconds. The range is 3 through 10 seconds.

See "About authentication settings on a Gateway appliance" on page 878.

To specify the frequency of challenge packets to be sent to clients

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the group of Enforcers.

The Enforcer group must include the Gateway Enforcer appliance for which you want to specify the frequency of challenge packets to be sent to clients.

4   Under **Tasks**, click **Edit Group Parameters**.

5   In the **Settings** dialog box, on the **Authentication** tab, under **Authentication Parameters**, type the maximum number of challenge packets that you want the Gateway Enforcer appliance to keep sending to a client during an authentication session in the **Time between packets in authentication session** field.

The default setting is 3 seconds. The range is from 3 through 10 seconds.

6   In the **Settings** dialog box, on the **Authentication** tab, click **OK**.

Specifying the time period for which a client is blocked after it fails authentication

You can specify the amount of time for which a client is blocked after it fails authentication.

The default setting is 30 seconds. The range is 10 through 300 seconds.

See "About authentication settings on a Gateway appliance" on page 878.

To specify the time period for which a client is blocked after it fails authentication

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the group of Enforcers.

The Enforcer group must include the Gateway Enforcer appliance for which you want to specify the amount of time that a client is blocked after it fails authentication.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Settings** dialog box, on the **Authentication** tab, under **Authentication Parameters**, type the number of seconds for the amount of time for which a client is blocked after it fails authentication in the **Time rejected client will be blocked (seconds)** field.

6   Click **OK**.

Specifying the time period for which a client is allowed to retain its network connection without reauthentication

You can specify the amount of time in seconds for which a client is allowed to retain its network connection without reauthentication.

The default setting is 30 seconds. The range is 10 through 300 seconds.

See "About authentication settings on a Gateway appliance" on page 878.

To specify the time period for which a client is allowed to retain its network connection without reauthentication

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

3 Under **Servers**, select and expand the group of Enforcers.

   The Enforcer group must include the Gateway Enforcer appliance for which you want to specify the amount of time that a client is blocked after it fails authentication.

4 Under **Tasks**, click **Edit Group Properties**.

5 In the **Settings** dialog box, on the **Authentication** tab, under **Authentication Parameters**, type the number of seconds for which a client is allowed to retain its network connection without reauthentication in the **Time authenticated client will be allowed (seconds)** field.

   The default setting is 30 seconds. The range is 10 through 300 seconds.

6 Click **OK**.

Allowing all clients with continued logging of non-authenticated clients

It can take some time to deploy all the client software. You may want to configure the Gateway Enforcer appliance to allow all clients to connect to the network until you have finished distributing the client package to all users. A Gateway Enforcer appliance blocks all clients that do not run the client. Because the client does not run on non-Windows operating systems such as Linux or Solaris, the Gateway Enforcer appliance blocks these clients. You have the option of allowing all non-Windows clients to connect to the network.

If a client is not authenticated with this setting, the Gateway Enforcer appliance detects the operating system type. Therefore Windows clients are blocked and non-Windows clients are permitted to access the network.

The default setting is not enabled.

Use the following guidelines when you apply the configuration settings:

- This setting should be a temporary measure because it makes the network less secure.

- While this setting is in effect, you can review Enforcer logs. You can learn about the types of clients that try to connect to the network at that location. For example, you can review the **Client Activity Log** to see if any of the clients do not have the client software installed. You can then make sure that the client software is installed on those clients before you disable this option.

See "About authentication settings on a Gateway appliance" on page 878.

To allow all clients with continued logging of non-authenticated clients

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

3 Select and expand the group of Enforcers.

   The Enforcer group must include the Gateway Enforcer appliance for which you want to allow all clients while continuing the logging of non-authenticated clients.

4 Under **Tasks**, click **Edit Group Properties**.

5 In the **Settings** dialog box, on the **Authentication** tab, check **Allow all clients, but continue to log which clients are not authenticated**.

   The default setting is not enabled.

6 In the **Settings** dialog box, on the **Authentications** tab, click **OK**.

Allowing non-Windows clients to connect to a network without authentication

The Gateway Enforcer appliance cannot authenticate a client that is running a non-Windows operating system. Therefore non-Windows clients cannot connect to the network unless you specifically allow them to connect to the network without authentication.

The default setting is not enabled.

You can use one of the following methods to enable the clients that support a non-Windows platform to connect to the network:

- Specify each non-Windows client as a trusted host.

- Allow all clients with non-Windows operating systems.

The Gateway Enforcer appliance detects the operating system of the client and authenticates Windows clients. However, it does not allow non-Windows clients to connect to the Gateway Enforcer appliance without authentication.

If you need to have non-Windows clients connect to the network, then you must configure additional settings on the Symantec Endpoint Protection Manager Console.

See

See

To allow non-Windows clients to connect to a network without authentication

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   In the **Admin** page, click **Servers**.

3   Under **Servers**, select and expand the group of Enforcers.

   The Enforcer group must include the Gateway Enforcer appliance for which you want to allow all non-Windows clients to connect to a network.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Settings** dialog box, on the **Authentication** tab, check **Allow all clients with non-Windows operating systems**.

   The default setting is not enabled.

6   Click **OK**.

Checking the policy serial number on a client

The Symantec Endpoint Protection Manager updates a client's policy serial number every time that the client's security policy changes. When a client connects to the Symantec Endpoint Protection Manager, it receives the latest security policies and the latest policy serial number.

When a client tries to connect to the network through the Gateway Enforcer appliance:

■ Retrieves the policy serial number from the Symantec Endpoint Protection Manager.

■ Compares the policy serial number with the one that it receives from the client.

■ If the policy serial numbers match, the Gateway Enforcer appliance has validated that the client is running an up-to-date security policy.

The default value for this setting is not enabled.

The following guidelines apply:

■ If the **Check the Policy Serial Number on Client before allowing Client into network** option is checked, a client must have the latest security policy before it can connect to the network through the Gateway Enforcer appliance. If the

client does not have the latest security policy, the client is notified to download the latest policy. The Gateway Enforcer appliance then forwards its Gateway request to receive a quarantine network configuration.

■ If the **Check the Policy Serial Number on Client before allowing Client into network** option is not checked and the Host Integrity check is successful, a client can connect to the network. The client can connect through the Gateway Enforcer appliance even if its security policy is not up-to-date.

See "About authentication settings on a Gateway appliance" on page 878.

To have the Gateway Enforcer appliance check the policy serial number on a client

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   In the **Admin** page, click **Servers**.

3   Select and expand the group of Gateway Enforcer appliances.

    The Enforcer group must include the Gateway Enforcer appliance that checks the Policy Serial Number on a client.

4   In the **Settings** dialog box, on the **Authentication** tab, check **Check the Policy Serial Number on the Client before allowing a Client into the network**.

5   Click **OK**.

Sending a message from a Gateway Enforcer appliance to a client about non-compliance

You can send a Windows pop-up message to inform a user that they cannot connect to the network. The message typically tells the user that a client cannot connect to the network because it does not run the Symantec Network Access Control client.

Most administrators type a brief statement of the need to run the Symantec Endpoint Protection client or the Symantec Network Access Control client. The message may include information about a download site where users can download the required client software. You can also provide a contact telephone number and other relevant information.

This setting is enabled by default. It applies only to clients that do not run the Symantec Endpoint Protection client or the Symantec Network Access Control client.

As soon as you complete this task, the pop-up message appears on the client if the Windows Messenger service is running on the client.

Note: Popup messages do not appear on Mac clients.

See "About authentication settings on a Gateway appliance" on page 878.

To send a message from a Gateway Enforcer appliance to a client about non-compliance

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

3 Select and expand the group of Enforcers.

4 Under **Tasks**, click **Edit Group Properties**.

5 In the **Settings** dialog box, on the **Authentication** tab, check **Enable pop-up message on Windows client if Client is not running**.

6 Click **Message**.

7 In the **Pop-up Message Settings** dialog box, select how often you want the message to appear on a client from the **Following message will pop up** list.

   You can select any of the following time periods:

   ■ Once
     The default value is Once.

   ■ Every 30 seconds

   ■ Every minute

   ■ Every 2 minutes

   ■ Every 5 minutes

   ■ Every 10 minutes

8 Type the message that you want to appear in the text box.

   The maximum number of characters is 125. This number includes spaces and punctuation.

   The default message is:

   ```
   You are blocked from accessing the network because you
   do not have the Symantec Client running. You will need to
   install it.
   ```

9 Click **OK**.

10 In the **Settings** dialog box, on the **Authentication** tab, click **OK**.

Redirecting HTTP requests to a Web page

The Gateway Enforcer appliance has an option to redirect HTTP requests to an internal Web server if the client tries to access an internal Web site through a browser and a client is not running on the client. If you do not specify a URL, the Gateway Enforcer appliance pop-up message appears as the HTML body for the first HTML page. You may want to connect users to a Web page that you set up. Clients can download Remediation software from this Web site. The Gateway Enforcer appliance can redirect the HTTP GET request to a URL that you specify.

This setting is enabled by default.

For example, you can redirect a request to a Web server from which the client can download the client software, patches, or up to date versions of applications.

See "About authentication settings on a Gateway appliance" on page 878.

To redirect HTTP requests to a Web page

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the group of Gateway Enforcer appliances.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Gateway Settings** dialog box, on the **Authentication** tab, check **Enable HTTP redirect on client if the client is not running**.

6   Type the URL in the HTTP redirect URL field.

    The host of the redirect URL must either be the Symantec Endpoint Protection Manager or an IP address that is listed as part of the internal trusted IP address range.

    The URL can have as many as 255 characters.

    If you want to specify a name of a Web server, you must also enable **Allow all DNS request packets** on the **Advanced** tab.

    If you leave the URL field empty and then click **OK**, the following message appears:

    ```
    The HTTP redirect URL must be a valid URL.
    ```

    This also uses the Gateway Enforcer pop-up message as the HTML body for the first HTML page it sends back to the client.

7   In the **Gateway Settings** dialog box, on the **Authentication** tab, click **OK**.

Authentication range settings

You can configure the following settings:

- Client IP addresses that the Gateway Enforcer appliance authenticate
  See "Adding client IP address ranges to the list of addresses that require authentication" on page 896.

- External IP addresses that the Gateway Enforcer appliance does not authenticate
  See "Specifying trusted external IP addresses" on page 899.

- Internal IP address to which the Gateway Enforcer allows access
  See "Adding a trusted internal IP address for clients on a management server" on page 898.

After you apply the settings, the changes are sent to the selected Gateway Enforcer appliance during the next heartbeat. Keep in mind the following information:

- The option to **Only authenticate clients with these IP addresses** is not selected by default. If you leave this option selected and do not specify any IP addresses to authenticate, the Gateway Enforcer appliance acts as a network bridge and allows all clients access.

- For **Trusted External IP address range addresses**, you should add the IP address of the corporate VPN server, as well as any other IP addresses that are allowed to have access to the corporate network without running a client. You may also want to include the devices that normally have access to the network and are running an operating system other than Windows.

- For **Trusted Internal IP address range addresses**, you may need to specify addresses, such as an update server, a file server containing antivirus signature files, a server that is used for remediation, or a DNS or WINS server that is required to resolve domain or host names.

- If you specify that the Gateway Enforcer appliance verifies that the client profile is up-to-date, clients may need to connect to the Symantec Endpoint Protection Manager to download the latest security policies. If you use this option when you refer to the Symantec Endpoint Protection Manager by DNS or host name, you must add the DNS or WINS server's IP address to the trusted internal IP list.

Client IP address ranges compared to trusted external IP addresses

The Client IP address range is similar to what is called a blacklist. You can specify the client IP addresses that tell the Gateway Enforcer appliance to only check specific IP addresses to see if they are running the client and meet required security

policies. If a client is not on the Client IP list, then it functions as if it had been assigned a trusted IP address.

In contrast to the Client IP address range, trusted external IP addresses are similar to what is called a white list. If you check **Assigning trusted external IP addresses**, the Gateway Enforcer appliance validates the client that tries to connect from the external side except clients with trusted external IP addresses. This process is the opposite of Client IP address range, which tells the Gateway Enforcer appliance to only validate the clients in the Client IP address range.

See "Adding client IP address ranges to the list of addresses that require authentication" on page 896.

When to use client IP address ranges

Client IP address range allows administrators to specify a range of IP addresses that represent the computers the Gateway Enforcer appliance must authenticate. Computers with addresses outside the Client IP address range are allowed to pass through the Gateway Enforcer appliance without requiring the client software or other authentication.

The reasons for using Client IP address ranges include:

- Allowing network access to external Web sites

- Authenticating a subset of clients

See "Adding client IP address ranges to the list of addresses that require authentication" on page 896.

Allowing network access to external Web sites

One reason for using Client IP address ranges is to allow network access to external Web sites from within your internal network. If an organization has computers on the corporate network that go out through the Gateway Enforcer appliance to access Web sites on the Internet, such as Symantec or Yahoo, the internal clients can query the Internet. However, the Gateway Enforcer appliance tries to authenticate the Web sites trying to respond to the client request.

Therefore internal clients connecting to the Internet through the Gateway Enforcer appliance are unable to access the Internet unless you configure the Client IP address range.

The Client IP address range may be all the IP addresses a VPN server would assign to any client.

For example, an internal client can access the Internet if Client IP address range is configured. When an internal user contacts a Web site, the site can respond to

the client because its IP address is outside the client IP address range. Therefore the internal user does not need to be authenticated.

See "Adding client IP address ranges to the list of addresses that require authentication" on page 896.

Authentication of a subset of clients

You may want to use client IP addresses to have a Gateway Enforcer appliance authenticate a limited subset of clients at a company.

You can have the Gateway Enforcer appliance check only those clients that connect through one subnet if you have already installed the clients on all of the computers. Other clients accessing the corporate network at that location are allowed to pass through without authentication. As the client is installed on other clients, you can add their addresses to the Client IP address range or use a different authentication strategy.

See "Adding client IP address ranges to the list of addresses that require authentication" on page 896.

About trusted IP addresses

You work with the following types of trusted IP addresses on a Gateway Enforcer:

■ Trusted external IP addresses
A trusted external IP address is the IP address of an external computer that is allowed to access the corporate network without running the client.
See "Specifying trusted external IP addresses" on page 899.

■ Trusted internal IP addresses
A trusted internal IP address is the IP address of a computer within the corporate network that any client can access from the outside.
See "Adding a trusted internal IP address for clients on a management server" on page 898.

You can add trusted IP addresses of both types on the Symantec Endpoint Protection Manager Console. Traffic to the console is always allowed from the Gateway Enforcer appliance.

Trusted external IP addresses

One of the primary duties of a Gateway Enforcer appliance is to check that all computers that try to access the network are running the client. Some computers may not be running the Windows operating system or may not be running the client.

For example, VPN and wireless servers do not typically run the client. In addition, a network setup may include the devices that normally access the network and run an operating system other than Windows. If these computers need to bypass a Gateway Enforcer appliance, you need to make sure that the Gateway Enforcer appliance knows about them. You can accomplish this objective by creating a range of trusted external IP addresses. In addition, you must also assign an IP address from that IP address range to a client.

See "Specifying trusted external IP addresses" on page 899.

Trusted internal IP addresses

A trusted internal IP address represents the IP address of a computer inside the corporate network that external clients can access from the outside. You can make certain internal IP addresses into trusted internal IP addresses.

When you specify trusted internal IP addresses, clients can get to that IP address from outside the corporate network whether or not:

■ The client software has been installed on the client computer

■ The client complies with a security policy

Trusted internal IP addresses are the internal IP addresses that you want users outside the company to be able to access.

Examples of the internal addresses that you may want to specify as trusted IP addresses are as follows:

■ An update server

■ A file server that contains antivirus signature files

■ A server that is used for remediation

■ A DNS server or a WINS server that is required to resolve domain or host names

When a client tries to access the internal network and does not get authenticated by the Gateway Enforcer appliance, the client can be placed in quarantine when:

■ The client is not running the client software on the client computer

■ The Host Integrity check failed

■ The client does not have an up-to-date policy

The client is still allowed to access certain IP addresses; these are the trusted internal IP addresses.

For example, the concept of trusted internal IP addresses may have an external client that needs to access the corporate network to get the client or other needed

software. The Gateway Enforcer appliance allows the external client to get to a computer that is on the list of trusted internal IP addresses.

See "Adding a trusted internal IP address for clients on a management server" on page 898.

Adding client IP address ranges to the list of addresses that require authentication

You can specify those clients with IP addresses to which the Gateway Enforcer appliance authenticates.

You want to be aware of the following issues:

- You must check the **Enable** option that is located next to the IP address or range if you want that address to be authenticated. If you want to temporarily disable authentication of an address or range, uncheck **Enable**.

- If you type an invalid IP address, you receive an error message when you try to add it to the Client IP list.

See "When to use client IP address ranges" on page 893.

To restrict a client's network access despite authentication

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the Gateway Enforcer appliance groups.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Gateway Settings** dialog box, on the **Auth Range** tab, in the **Authenticate Client IP address range** area, check **Only authenticate clients with these IP addresses**.

    If you do not check this option, any IP addresses listed are ignored. Therefore all clients who try to connect to the network are authenticated. If you check this option, the Gateway Enforcer appliance authenticates only the clients with the IP addresses that are added to the list.

6   Click **Add**.

7   In the **Add Single IP Address** dialog box, select **from Single IP address to IP address range or Subnet**.

    The fields change to enable you to enter the appropriate information.

8   Select whether to add:

    - A single IP address

- An IP address range

- An IP address plus subnet mask

9 Type either a single IP address, a start address and an end address of a range, or an IP address plus subnet mask.

10 Click **OK**.

The address information you typed is added to the Client IP address range table, with the **Enable** option selected.

11 Continue to click **Add** and specify any other IP addresses or ranges of addresses that you want the Gateway Enforcer to authenticate.

12 Click **OK**.

Editing client IP address ranges on the list of addresses that require authentication

You may need to edit client IP address ranges that you want to be authenticated.

See "When to use client IP address ranges" on page 893.

To edit client IP address ranges on the list of addresses that require authentication

1 In Symantec Endpoint Protection Manager, click **Admin**.

2 Click **Servers**.

3 Select and expand the group of Enforcers.

4 Select the group of Enforcers for which you want to edit client IP address ranges on the list of addresses that require authentication.

5 Under **Tasks**, click **Edit Group Properties**.

6 In the **Gateway Settings** dialog box, on the **Auth Range** tab, in the **Client IP address range** area, click anywhere in the column of IP addresses and click **Edit all**.

7 Click **OK**.

8 In the **Gateway Settings** dialog box, click **OK**.

Removing client IP address ranges from the list of addresses that require authentication

You may need to remove client IP address ranges.

See "When to use client IP address ranges" on page 893.

To remove client IP address ranges from the list of addresses that require authentication

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the group of Enforcers.

4   Select the group of Gateway Enforcer appliances for which you want to edit client IP address ranges on the list of addresses that require authentication.

5   Under **Tasks**, click **Edit Group Properties**.

6   In the **Gateway Settings** dialog box, on the **Auth Range** tab, in the **Client IP address range** area, click the row containing the IP address that you want to remove.

7   Click **Remove**.

8   Click **OK**.

Adding a trusted internal IP address for clients on a management server

The Trusted Internal IP table has a list of internal IP addresses that external clients are allowed to communicate with, regardless of whether a client currently runs or has passed the Host Integrity check.

If you run two Gateway Enforcer appliances in a series so that a client connects through more than one Gateway Enforcer appliance, the Gateway Enforcer appliance closest to the Symantec Endpoint Protection Manager needs to be specified as a trusted internal IP address of the other Gateway Enforcer appliances. If a client first fails a Host Integrity check and then passes it, you may have up to a 5-minute delay before a client can connect to the network.

See "About trusted IP addresses" on page 894.

To add a trusted internal IP address for clients on a management server

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   In the **Admin** page, click **Servers**.

3   Select and expand the group of Enforcers.

4   Select the Gateway Enforcer appliance group for which you want to edit client IP address ranges on the list of addresses that require authentication.

5   Under **Tasks**, click **Edit Group Properties**.

6   In the **Gateway Settings** dialog box, on the **Auth Range** tab, in the **Trusted IP address range** area, select **Trusted Internal IP address range** from the drop-down list.

7   Click **Add**.

8   In the **IP Address Settings** dialog box, type an IP address or address range.

9   Click **OK**

    The IP address is added to the list and a check mark appears in the Enable column.

10 In the **Settings** dialog box, click **OK**.

Specifying trusted external IP addresses

If you add trusted external IP addresses, the Gateway Enforcer appliance allows clients at these IP addresses to connect to the network even if they do not run any client software.

Because a client is not installed on VPN servers, you should add the server IP to the trusted IP list if you have a VPN server requiring network access through a Gateway Enforcer.

If you enter an invalid IP address, you receive an error message.

Note: You need to add the corporate VPN server's internal IP address in the Trusted external IP Addresses field first.

See "About trusted IP addresses" on page 894.

To specify trusted external IP addresses

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the group of Enforcers.

4   Select the group of Enforcers for which you want to specify trusted external IP addresses.

5   Under **Tasks**, click **Edit Group Properties**.

6   In the **Gateway Settings** dialog box, on the **Auth Range** tab, in the **Trusted IP address range** area, select **Trusted External IP address range** from the drop-down list.

7   Click **Add**.

8   In the **IP Address Settings** dialog box , type an IP address or address range.

9   Click **OK**.

The IP address is added to the list and a check mark appears in the **Enable** column.

10   In the **Settings** dialog box, click **OK**.

Editing trusted internal or external IP address

You may need to edit trusted internal as well as external IP addresses.

See "About trusted IP addresses" on page 894.

To edit a trusted internal or external IP address

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the group of Enforcers.

4   Select the group of Enforcers for which you want to edit a trusted internal or external IP address.

5   Under **Tasks**, click **Edit Group Properties**.

6   In the **Gateway Settings** dialog box, on the **Auth Range** tab, in the **Trusted IP address range** area, select **Trusted Internal IP address range** or **Trusted External IP address range** from the drop-down list.

The addresses for the selected type appear in the table.

7   In the **Trusted IP address range** table, click anywhere in the column of IP addresses and click **Edit all**.

8   In the **IP Address Editor** dialog box, locate any addresses you want to change and edit them.

9   Click **OK**.

10   In the **Settings** dialog box, click **OK**.

Removing a trusted internal or trusted external IP address

If you no longer want to allow external users who are not fully authenticated to have access to a particular internal location, remove the IP address from the Trusted Internal IP Address table.

See "About trusted IP addresses" on page 894.

To remove a trusted internal IP or trusted external IP address

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

3 Select and expand the Gateway Enforcer appliance group.

4 Select the group of Gateway Enforcer appliances for which you want to remove a trusted internal IP or trusted external IP address.

5 Under **Tasks**, click **Edit Group Properties**.

6 In the **Gateway Settings** dialog box, on the **Auth Range** tab, in the **Trusted IP address range** area, select **Trusted Internal IP address range** or **Trusted External IP address range** from the drop-down list.

The addresses for the selected type appear in the table.

7 In the table, click the row containing the IP address that you want to remove.

8 Click **Remove**.

9 In the **Settings** dialog box, click **OK**.

IP address range checking order

If both Client IP address range and trusted internal IP addresses are in use, the Gateway Enforcer appliance checks client addresses in the following order when a packet is received from a client:

■ If the Client IP address range is enabled, the Gateway Enforcer appliance checks the Client IP address range table for an address matching the source IP of the client.

■ If the Client IP address range does not include an IP address for that client, the Gateway Enforcer appliance allows the client without authentication.

■ If the Client IP address range does include an IP address for that client, the Gateway Enforcer appliance next checks the trusted external IP address range for a matching address.

■ If an address matching the client is found in the trusted external IP address range, the Gateway Enforcer appliance allows the client.

■ If no matching address is found in the trusted external IP address range, the Gateway Enforcer appliance then checks the destination address against the trusted internal IP address range list and the list of instances of the Symantec Endpoint Protection Manager.
If a matching address is still not located, the Gateway Enforcer appliance begins the authentication session and sends the challenge packet.

See "Specifying trusted external IP addresses" on page 899.

See "Adding client IP address ranges to the list of addresses that require authentication" on page 896.

About advanced Gateway Enforcer appliance settings

You can configure the following advanced Gateway Enforcer appliance configuration settings:

■ Allow all DHCP request packets.

■ Allow all DNS request packets.

■ Allow all ARP request packets.

■ Allow other protocols besides IP and ARP.
  You can specify the types of protocols that you want to allow in the Filter field.
  See "Specifying packet types and protocols" on page 902.

■ Allow legacy clients
  See "Allowing a legacy client to connect to the network with a Gateway Enforcer appliance" on page 904.

■ Enable local authentication
  See "Enabling local authentication on a Gateway Enforcer appliance" on page 904.

■ Enable system time updates for Gateway Enforcer appliance clients
  See "Enabling system time updates for the Gateway Enforcer appliance using the Network Time Protocol" on page 905.

■ Use the Gateway Enforcer as a Web server
  See "Using the Gateway Enforcer appliance as a Web server" on page 905.

■ Use the Gateway Enforcer as a DNS spoofing server
  See "Using the Gateway Enforcer as a DNS spoofing server " on page 906.

When you apply the settings, the changes that have been made are sent to the selected Gateway Enforcer appliance during the next heartbeat.

Specifying packet types and protocols

You can specify that the Gateway Enforcer appliance allows certain packet types to pass through without requiring a client to run or require authentication.

See "About advanced Gateway Enforcer appliance settings" on page 902.

To specify packet types and protocols

1   In the Symantec Endpoint Protection Manager, click **Admin**.

2   In the **Admin** page, click **Servers**.

3   Select and expand the Gateway Enforcer appliance group.

4   Select the group of Gateway Enforcer appliances for which you want to specify packet types and protocols.

5   Under **Tasks**, click **Edit Group Properties**.

6   In the **Gateway Settings** dialog box, on the **Advanced** tab, check or uncheck the following packet types or protocols:

   ■ **Allow all DHCP request packets**
   When enabled, the Gateway Enforcer appliance forwards all DHCP requests from the external network into the internal network. Because disabling this option prevents the client from getting an IP address, and since the client requires an IP address to talk to a Gateway Enforcer appliance, it is recommended that this option remain enabled.
   The default setting is enabled.

   ■ **Allow all DNS request packets**
   When enabled, the Enforcer forwards all DNS requests from the external network into the internal network. This option must be enabled if the client is configured to communicate with the Symantec Endpoint Protection Manager by name rather than by IP address. This option must also be enabled if you want to use the **HTTP redirect requests** option on the **Authentication** tab.
   The default setting is enabled.

   ■ **Allow all ARP request packets**
   When this option enabled, the Gateway Enforcer appliance allows all ARP packets from the internal network. Otherwise the Gateway Enforcer appliance treats the packet as a normal IP packet and uses the sender IP as source IP and target IP as destination IP and carries out the authentication process.
   The default setting is enabled.

   ■ **Allow other protocols besides IP and ARP**
   When this option is enabled, the Gateway Enforcer appliance forwards all packets with other protocols. Otherwise it drops them.
   The default setting is disabled.
   If you checked **Allow other protocols besides IP and ARP**, you may want to complete the **Filter** field. You can hover over the field to see examples, some of which follow.

Examples: `allow 800, 224.12.21,900-90d, 224.21.20-224-12.21.100;`
`block 810,224.12.21.200`

7 Click **OK**.

Allowing a legacy client to connect to the network with a Gateway Enforcer appliance

You can enable a Gateway Enforcer appliance to connect to 5.1.x legacy clients.
If your network supports an 11.0.2 Symantec Endpoint Protection Manager, a
Symantec Gateway Enforcer appliance, and needs to support 5.1.x legacy clients,
you can enable the support of 5.1.x legacy clients on the management server
console so that the Symantec Gateway Enforcer appliance does not block them.

See "About advanced Gateway Enforcer appliance settings" on page 902.

To allow a legacy client to connect to the network with a Gateway Enforcer appliance

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

3 Select and expand the group of Gateway Enforcers appliances.

4 Under **Tasks**, click **Edit Group Properties**.

5 In the Settings dialog box, on the **Advanced** tab, check **Allow legacy clients**.

6 Click **OK**.

Enabling local authentication on a Gateway Enforcer appliance

With local authentication enabled, the Gateway Enforcer appliance loses its
connection with the server on which the Symantec Endpoint Protection Manager
is installed. Therefore the Gateway Enforcer appliance authenticates a client
locally.

See "About advanced Gateway Enforcer appliance settings" on page 902.

To enable local authentication on a Gateway Enforcer appliance

1 In Symantec Endpoint Protection Manager, click **Admin**.

2 Click **Servers**.

3 Select and expand the group of Gateway Enforcers appliances.

4 Under **Tasks**, click **Edit Group Properties**.

5   In the **Settings** dialog box, on the **Advanced** tab, check **Enable Local Authentication**.

6   Click **OK**.

Enabling system time updates for the Gateway Enforcer appliance using the Network Time Protocol

With Network Time Protocol (NTP) enabled, Gateway Enforcer appliance clocks can update to the correct time. This setting is disabled by default, but it can be overridden if it is specified in a group policy.

See "About advanced Gateway Enforcer appliance settings" on page 902.

To enable time updates for Gateway Enforcer appliance from the Symantec Endpoint Protection Manager

1   In the Symantec Endpoint Protection Manager, click **Admin**.

2   In the **Admin** page, click **Servers**.

3   Under **Servers**, select and expand the group of Gateway Enforcer appliances.

4   Under **Tasks**, click **Edit Group Properties**.

5   On the **Advanced** tab, check **Enable Network Time Protocol**.

6   Enter the IP address or the fully qualified domain name of the NTP server.

7   Click **OK**.

From the Enforcer console, you can temporarily change this setting to help troubleshoot time synchronization issues. From the Enforcer console command line, enter Enforcer (configure)**# ntp**.

Using the Gateway Enforcer appliance as a Web server

You can use the Gateway Enforcer appliance as a Web server which communicates with Symantec Endpoint Protection Manager and serves On-Demand agents. As a Web server, the Enforcer stops forwarding non-Enforcer local traffic from internal and external network but it continues to communicate with the Symantec Endpoint Protection Manager. The ability to act as a Web server is especially useful in 802.1x environments when you want to deploy the Enforcer on a VLAN and serve On-Demand clients to guest users

To use the Gateway Enforcer appliance as a Web server, you disable guest enforcement. You can enable guest enforcement when you want to switch back to using the Gateway Enforcer appliance to enforce guest access.

See "About advanced Gateway Enforcer appliance settings" on page 902.

To use the Gateway Enforcer appliance as a Web server

1   Log on to the Gateway Enforcer appliance as a superuser.

2   Type the following command:

   Enforcer#**configure advanced**

3   Type the following command:

   Enforcer (advanced)#**guest-enf disable**

To enable guest enforcement, type the following command:

Enforcer(advanced)# **guest_enf enable**

To check the status of guest enforcement, type the following command:

Enforcer(advanced)# **show status**

Status can be OFFLINE or ONLINE with an ACTIVE, STANDBY, or GUEST ENFORCEMENT status.

Using the Gateway Enforcer as a DNS spoofing server

When guest enforcement is enabled, the Gateway Enforcer provides DNS spoofing functionality. You cannot use this feature unless guest enforcement is enabled.

The enabled mode routes URL requests to the Gateway Enforcer instead of a remediation Web site. To activate this functionality, you must provide an IP address as the answer in a DNS response packet.

See

To use the Gateway Enforcer as a DNS spoofing server

1   Log on to the Gateway Enforcer appliance as a superuser.

2   Type the following command:

   Enforcer#**configure advanced**

3 Type the following command:

Enforcer (advanced)# **dns-spoofing enable** |*use_local_ip* | *dns_spoofing_ip*

4 You can use the Gateway Enforcer's IP address or set a custom IP address.

To use the Gateway Enforcer's IP address	Enforcer (advanced)# **dns-spoofing use-local-ip enable**
To set a custom IP address	Enforcer (advanced)# **dns-spoofing-ip** *IP_ADDRESS* Where: *IP_ADDRESS* is your selected IP address

To disable DNS spoofing, type the following command:

Enforcer (advanced)# **dns-spoofing disable**

To check DNS spoofing status, type the following command:

Enforcer (advanced)# **show**

The status shows the DNS spoofing feature as ENABLED or DISABLED.

Installation planning for the LAN Enforcer appliance

This chapter includes the following topics:

- Planning for the installation of a LAN Enforcer appliance
- Failover planning for LAN Enforcer appliances and RADIUS servers

Planning for the installation of a LAN Enforcer appliance

The LAN Enforcer appliance can perform host authentication and act as a pseudo-RADIUS server (even without a RADIUS server). The Enforcement client acts as an 802.1x supplicant. It responds to the switch's Extensible Authentication Protocol (EAP) challenge with the Host Integrity status and policy number information. The RADIUS server IP address is set to 0 in this case, and no traditional EAP user authentication takes place. The LAN Enforcer appliance checks Host Integrity. It can allow, block, or dynamically assign a VLAN, based on the results of the Host Integrity check.

Another configuration is also available. You can use a LAN Enforcer appliance with a RADIUS server to enforce 802.1x EAP authentication internally in a corporate network. If a LAN Enforcer appliance is used in this configuration, you need to position it so that it can communicate with the RADIUS server.

If your switch supports dynamic VLAN switching, additional VLANs can be configured on the switch and accessed through the LAN Enforcer appliance. The switch can dynamically put the client into a VLAN that is based on the reply from the LAN Enforcer appliance. You may want to add VLANs for quarantine and remediation.

Several types of planning information can help you implement LAN Enforcer appliances in a network.

Note: Note: If you are upgrading from Symantec Sygate Endpoint Protection 5.1 clients, you must upgrade Symantec Endpoint Protection Manager first, then your Enforcers, then your clients, moving them to version 11.x first. Once you have Symantec Endpoint Protection Manager and your Enforcers at version 11.x, you must check **Allow Legacy Clients** on the Enforcer menu before you take the final step. Then finish the upgrade to the current release.

See "Where to place LAN Enforcer appliances" on page 910.

Where to place LAN Enforcer appliances

A LAN Enforcer appliance acts as a RADIUS proxy. Administrators typically use a LAN Enforcer appliance with a RADIUS server to enforce 802.1x Extensible Authentication Protocol (EAP) authentication in a corporate network. If you use a LAN Enforcer appliance in this configuration, the LAN Enforcer appliance must be able to communicate with the RADIUS server.

For example, you can connect a LAN Enforcer appliance to an 802.1x-aware LAN switch on an internal VLAN with a Symantec Endpoint Protection Manager, RADIUS server, and clients. A computer that does not have the client software cannot connect to the network. However, the client is directed to a remediation server from which it can obtain the software that it needs to become compliant.

See "Setting up an Enforcer appliance" on page 803.

Figure 48-1 shows an example of where you can place a LAN Enforcer appliance in the overall internal network configuration.

Figure 48-1   Placement of LAN Enforcer appliances
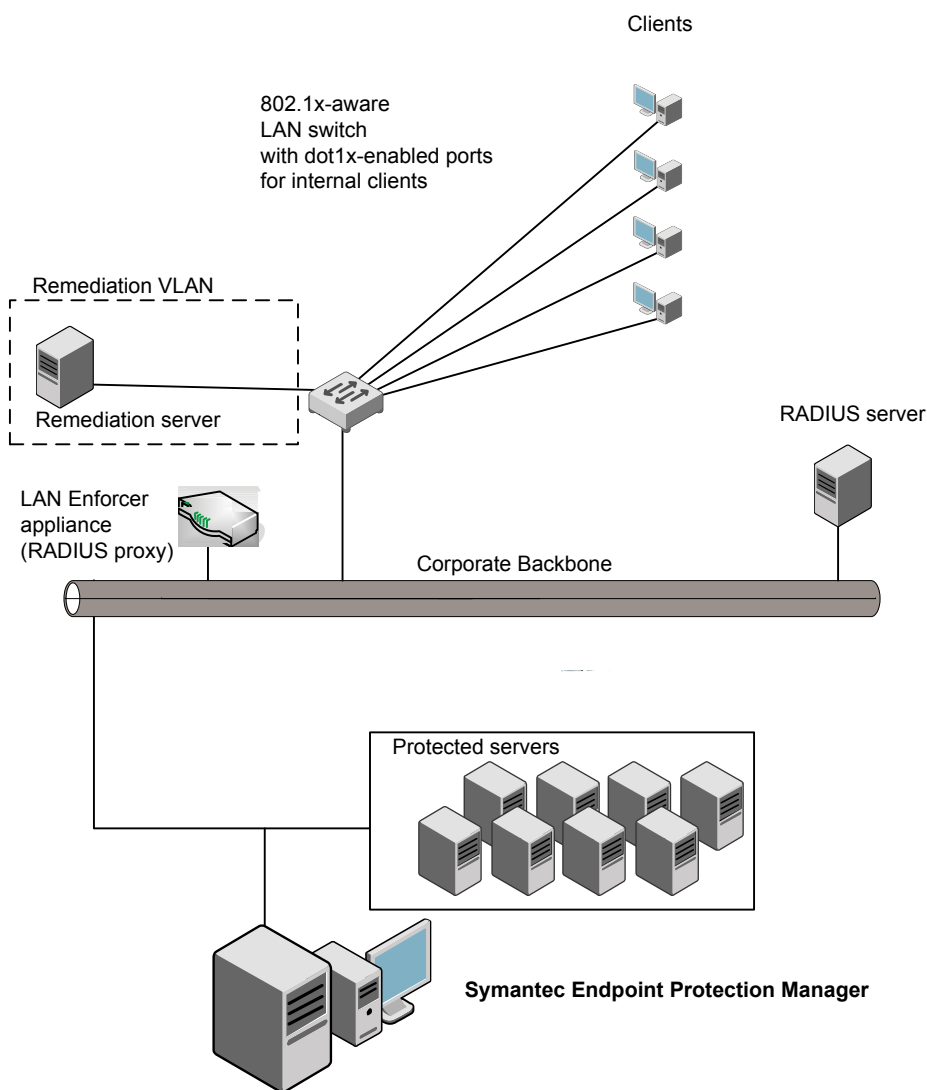
If a switch supports dynamic VLAN switching, additional VLANs can be configured on the 802.1x-aware switch and accessed through the LAN Enforcer appliance. The 802.1x-aware switch can dynamically put the client into a VLAN after it receives a reply from the RADIUS server. Some 802.1x-aware switches also include a default VLAN or guest VLAN feature. If a client has no 802.1x supplicant, the 802.1x-aware switch can put the client into a default VLAN.

You can install the LAN Enforcer appliance so that you can enable EAP authentication throughout the network with the equipment that is already deployed. LAN Enforcer appliances can work with existing RADIUS servers , 802.1x supplicants, and 802.1x-aware switches. They perform the computer level authentication. It makes sure that the client complies with security policies.

For example, it checks that antivirus software has been updated with the latest signature file updates and the required software patches. The 802.1x supplicant and the RADIUS server perform the user-level authentication. It authenticates the clients who try to connect to the network are the ones who they claim to be.

Alternatively, a LAN Enforcer appliance can also work in transparent mode, removing the need for a RADIUS server. In transparent mode, the client passes Host Integrity information to the 802.1x-aware switch in response to the EAP challenge. The switch then forwards that information to the LAN Enforcer. A LAN Enforcer appliance then sends authentication results back to the 802.1x-aware switch. The information that the LAN Enforcer appliance sends is based on the Host Integrity validation results. Therefore the LAN Enforcer appliance requires no communication with a RADIUS server.

The following configurations are available for a LAN Enforcer appliance:

■ Full 802.1x mode
  This configuration requires a RADIUS server and third-party 802.1x supplicants. Both traditional EAP user authentication and Symantec Host Integrity validation are performed.

■ Transparent mode
  This configuration does not require a RADIUS server or the use of a third-party 802.1x supplicants. Only Host Integrity validation is performed.

You can consider the following issues:

■ Do you have clients such as printers and IP phones that do not have 802.1x supplicants running on them?
  Consider using MAB authentication.

■ Do you have client such as printers and IP phones that have custom 802.1x supplicants running on them?
  Consider configuring the ignore Symantec NAC Client checking.

■ Do you plan to have an 802.1x supplicant installed on every computer?
  If you plan to have an 802.1x supplicant installed on every computer, you can use the Full 802.1x mode.

■ Do you want to perform a user level authentication in addition to the Host Integrity check?
  If you want to perform a user level authentication in addition to the Host Integrity check, you must use the Full 802.1x mode.

■ Do you plan to use a RADIUS server in a network configuration?
If you plan to use a RADIUS server in a network configuration, you can use either the Full 802.1x mode or transparent mode. If you do not plan to use a RADIUS server in a network configuration, you must use the transparent mode.

Failover planning for LAN Enforcer appliances and RADIUS servers

If you have installed two LAN Enforcer appliances in a network, failover is handled through the 802.1x-aware switch. An 802.1x-aware switch can support multiple LAN Enforcer appliances. You can easily synchronize the settings of LAN Enforcer appliances on the Symantec Endpoint Protection Manager through the use of synchronization settings.

If you want to synchronize the settings of one LAN Enforcer appliance with another LAN Enforcer appliance, specify the same group Enforcer name on the Enforcer console.

If you use a RADIUS server in your network, provide for RADIUS server failover by configuring the LAN Enforcer appliance to connect to multiple RADIUS servers. If all the RADIUS servers that are configured for that LAN Enforcer appliance become disabled, the switch assumes that the LAN Enforcer appliance is disabled. Therefore, the 802.1x-aware switch connects to a different LAN Enforcer appliance that provides additional failover support.

See "Configuring an Enforcer appliance" on page 805.

Where to place RADIUS servers for failover in a network

Figure 48-2 describes how to provide failover for LAN Enforcer appliances.

Figure 48-2   Placement of two RADIUS servers
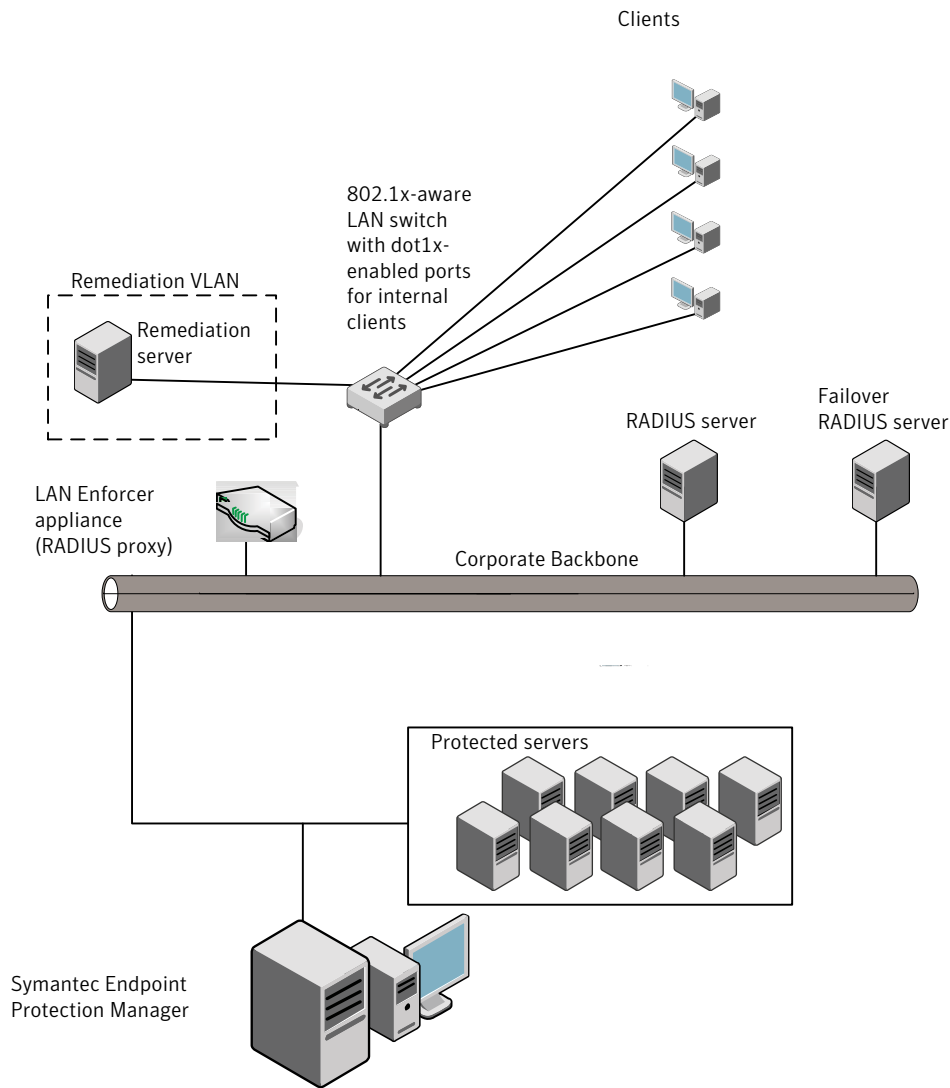
See

Configuring the LAN Enforcer appliance on the Symantec Endpoint Protection Manager

This chapter includes the following topics:

About configuring the Symantec LAN Enforcer on the Symantec Endpoint Protection Manager Console

You can add or edit the configuration settings for the LAN Enforcer in the Symantec Endpoint Protection Manager console. The Symantec Endpoint Protection Manager is also referred to as the management server.

Before you can proceed, you must complete the following tasks:

■ Install the software for the Symantec Endpoint Protection Manager on a computer.
See "Installing Symantec Endpoint Protection Manager" on page 95.
The computer on which the Symantec Endpoint Protection Manager software is installed is also referred to as the management server.

■ Connect the Symantec LAN Enforcer appliance to the network.
See "Setting up an Enforcer appliance" on page 803.

■ Configure the Symantec LAN Enforcer appliance on the local LAN Enforcer console during the installation.
See "Changing LAN Enforcer configuration settings in Symantec Endpoint Protection Manager" on page 920.

After you finish these tasks, you can specify all additional configuration settings for the LAN Enforcer appliance on a management server.

About configuring RADIUS servers on a LAN Enforcer appliance

You can modify the LAN Enforcer settings in the Symantec Endpoint Protection console. The Enforcer must be installed and connected to the Symantec Endpoint Protection Manager before you can configure it to enforce Host Integrity policies on the client.

You can configure the following options for the LAN Enforcer:

■ Define the Enforcer group description, listen port, and management server list.

■ Configure the RADIUS server Group. You configure the host name or IP address, authentication port, timeout, shared secret, and number of retransmits. If you configure multiple servers in the group and one goes down, the LAN Enforcer connects to the next server in the list.

■ Configure a switch or group of switches.

■ Settings for enabling logging and specifying log file parameters.

■ Enable and disable local authentication and legacy clients.

■ Configure the LAN Enforcer working as an NTP client.

If a setting refers to an 802.1x-aware switch, the same instructions apply to configuring wireless access points.

See "About configuring 802.1x wireless access points on a LAN Enforcer appliance" on page 919.

About configuring 802.1x wireless access points on a LAN Enforcer appliance

The LAN Enforcer appliance supports a number of wireless protocols, which includes WEP 56, WEP 128, and WPA/WPA2 with 802.1x.

You can configure a LAN Enforcer to protect the wireless access point (AP) as much as it protects a switch if the following conditions are met:

■ The network includes a wireless LAN Enforcer appliance with 802.1x.

■ Wireless clients run a supplicant that supports one of these protocols.

■ The wireless AP supports one of these protocols.

For wireless connections, the authenticator is the logical LAN port on the wireless AP.

You configure a wireless AP for 802.1x and for switches in the same way. You include wireless APs to the LAN Enforcer settings as part of a switch profile. Wherever an instruction or part of the user interface refers to a switch, use the comparable wireless AP terminology. For example, if you are instructed to select a switch model, select the wireless AP model. If the vendor of the wireless AP is listed, select it for the model. If the vendor is not listed, choose **Others**.

The configuration for wireless AP for 802.1x and for switches include the following differences:

■ Only basic configuration is supported.
The transparent mode is not supported.

■ There can also be differences in support for VLANs, depending on the wireless AP.
Some dynamic VLAN switches may require you to configure the AP with multiple service set identifiers (SSIDs). Each SSID is associated with a VLAN.
See the documentation that comes with the dynamic VLAN switch.

Based on the wireless AP model that you use, you may want to use one of the following access control options instead of a VLAN:

Access control lists (ACLs)	Some wireless APs support ACLs that enable the network administrator to define policies for network traffic management. You can use the generic option on the LAN Enforcer by selecting the vendor name of the wireless AP. As an alternative, you can select **Others** for the 802.1x-aware switch model (if it is not listed).
	The generic option sends a generic attribute tag with the VLAN ID or name in it to the access point. You can then customize the access point. Now the access point can read the generic attribute tag for the VLAN ID and match it with the WAP's ACL ID. You can use the Switch Action table as an ACL Action table.
	Additional configuration on the wireless AP or AP controller may be required. For example, you may need to map the RADIUS tag that is sent to the wireless AP on the AP controller.
	See the wireless AP documentation for details.
MAC level 802.1x	You can plug the wireless AP into a switch that supports MAC level 802.1x. For this implementation, you must disable 802.1x on the wireless AP. You can only use it on the switch. The switch then authenticates the wireless clients by recognizing the new MAC addresses. After it authenticates a MAC address, it puts that MAC address on the specified VLAN instead of the whole port. Every new MAC address has to be authenticated. This option is not as secure. However, this option enables you to use the VLAN switching capability.

Changing LAN Enforcer configuration settings in Symantec Endpoint Protection Manager

You can change the LAN Enforcer configuration settings on a management server. The configuration settings are automatically downloaded from the management server to the LAN Enforcer appliance during the next heartbeat.

To change LAN Enforcer configuration settings in Symantec Endpoint Protection Manager

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3 Select the group of Enforcers of which the LAN Enforcer appliance is a member.

The Enforcer group must include the LAN Enforcer whose configuration settings need to be changed.

4 Select the LAN Enforcer appliance whose configuration settings need to be changed.

5 Under **Tasks**, click **Edit Group Properties**.

6 In the **Settings** dialog box, change any of the configuration settings.

The **LAN Enforcer Settings** dialog box provides the following categories of configuration settings:

General	This tab provides the following LAN Enforcer settings: ■ Group name for LAN Enforcer appliances ■ Listening port ■ Description for the LAN Enforcer appliance group ■ Selection of the management server list that the LAN Enforcer uses See "Using general settings" on page 922.
RADIUS Server Group	This tab provides the following LAN Enforcer settings: ■ Name for the RADIUS Server group ■ Host name or IP address for the RADIUS Server ■ Port number for the RADIUS Server ■ Friendly name for the RADIUS Server See "Using RADIUS server group settings" on page 926.
Switch	This tab provides the following LAN Enforcer settings: ■ Enable the switch policy ■ The name of the switch policy ■ The switch model, selected from a list of supported switches ■ The shared secret ■ The RADIUS server group ■ The reauthentication timeout period ■ Whether the switch forwards other protocols besides EAP ■ Switch Address ■ The VLAN on the Switch ■ Action See "Using switch settings" on page 933.

Advanced	This tab provides the following advanced LAN Enforcer settings:
	■ Configure Mac Authentication Bypass (MAB)
	■ Specify MAC addresses and VLANs
	■ Allow legacy client
	■ Enable local authentication
	■ Configure Network Time Protocol
	See "Using advanced LAN Enforcer appliance settings" on page 958.
Log settings	Settings for enabling logging of Server logs, Client Activity logs, and specifying log file parameters.
	See "About Enforcer reports and logs" on page 976.
	See "Configuring Enforcer log settings" on page 977.

Using general settings

You can add or edit the description of a LAN Enforcer appliance or a LAN Enforcer appliance group in the Symantec Endpoint Protection Manager Console.

See "Adding or editing the description of an Enforcer group with a LAN Enforcer" on page 924.

See "Adding or editing the description of a LAN Enforcer" on page 924.

You must establish a listening port that is used for communication between the VLAN switch and the LAN Enforcer appliance.

See "Specifying a listening port for communication between a VLAN switch and a LAN Enforcer" on page 923.

However, you cannot add or edit the name of a LAN Enforcer appliance group in the Symantec Endpoint Protection Manager Console. You cannot add or edit the IP address or host name of a LAN Enforcer appliance in the Symantec Endpoint Protection Manager Console. Instead, you must perform these tasks on the Enforcer console.

See "Adding or editing the name of a LAN Enforcer appliance group with a LAN Enforcer" on page 923.

However, you can only change the IP address or host name of a LAN Enforcer on the Enforcer console during the installation. If you later want to change the IP address or host name of a LAN Enforcer, you can do so on the LAN Enforcer console.

See "Adding or editing the IP address or host name of a LAN Enforcer" on page 924.

However, you can add or edit the IP address or host name of a Symantec Endpoint Protection Manager in a management server list.

See "Connecting the LAN Enforcer to a Symantec Endpoint Protection Manager" on page 925.

Adding or editing the name of a LAN Enforcer appliance group with a LAN Enforcer

You cannot add or edit the name of a LAN Enforcer appliance group of which a LAN Enforcer appliance is a member. You perform these tasks on the Enforcer console during the installation. If you later want to change the name of a LAN Enforcer appliance group, you can do so on the Enforcer console.

All Enforcers in a group share the same configuration settings.

See "Using general settings" on page 922.

Specifying a listening port for communication between a VLAN switch and a LAN Enforcer

When you configure the settings for a LAN Enforcer you specify the following listening ports:

■ The listing port that is used for communication between the VLAN switch and the LAN Enforcer.
   The VLAN switch sends the RADIUS packet to the UDP port.

■ The listening port that is used for communication between the LAN Enforcer and a RADIUS server.
   You specify this port when you specify a RADIUS server.

If the RADIUS server is installed on the management server, it should not be configured to use port 1812. The RADIUS servers are configured to use port 1812 as the default setting. Because the management server also uses port 1812 to communicate with the LAN Enforcer, there is a conflict.

See "Using general settings" on page 922.

To specify a listening port that is used for communication between a VLAN switch and a LAN Enforcer

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **Servers**, select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Setting**s dialog box, on the **General** tab, type the number of the UDP port that you want to assign in the **Listen port** field.

The default setting for the port is 1812. The range extends from 1 through 65535.

6   Click **OK**.

Adding or editing the description of an Enforcer group with a LAN Enforcer

You can add or edit the description of an Enforcer group of which a Symantec LAN Enforcer appliance is a member. You can perform this task on the Symantec Endpoint Protection Manager console instead of the LAN Enforcer console.

See "Using general settings" on page 922.

To add or edit the description of an Enforcer group with a LAN Enforcer

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the Enforcer group whose description you want to add or edit.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Settings** dialog box, on the **General** tab, add or edit a description for the Enforcer group in the **Description** field.

6   Click **OK**.

Adding or editing the IP address or host name of a LAN Enforcer

You can only change the IP address or host name of a LAN Enforcer on the Enforcer console during the installation. If you later want to change the IP address or host name of a LAN Enforcer, you can do so on the LAN Enforcer console.

See "Using general settings" on page 922.

Adding or editing the description of a LAN Enforcer

You can add or edit the description of a LAN Enforcer. You can perform this task on the Symantec Endpoint Protection Manager console instead of the LAN Enforcer console. After you complete this task, the description appears in Description field of the Management Server pane.

See "Using general settings" on page 922.

To add or edit the description of a LAN Enforcer

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

3 Select and expand the Enforcer group that includes the LAN Enforcer whose description you want to add or edit.

4 Select the LAN Enforcer whose description you want to add or edit.

5 Under **Tasks**, click **Edit Enforcer Properties**.

6 In the **Enforcer Properties** dialog box, add or edit a description for the LAN Enforcer in the **Description** field.

7 Click **OK**.

Connecting the LAN Enforcer to a Symantec Endpoint Protection Manager

Enforcers must be able to connect to servers on which the Symantec Endpoint Protection Manager is installed. The Symantec Endpoint Protection Manager uses a management server list to help manage the traffic between clients, management servers, and optional Enforcers, such a LAN Enforcer. The management server list specifies to which Symantec Endpoint Protection Manager a LAN Enforcer connects. It also specifies to which Symantec Endpoint Protection Manager a LAN Enforcer connects in case of a management server's failure.

If an administrator has created multiple management server lists, you can select the specific management server list that includes the IP addresses or host names of those management servers to which you want the LAN Enforcer to connect. If there is only one management server at a site, then you can select the default management server list. You can also select the management server list that you want an Enforcer group to be able to roam among, making choices in the same dialog box.

See "Using general settings" on page 922.

See "Configuring a management server list" on page 740.

To connect the LAN Enforcer to a Symantec Endpoint Protection Manager

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

3 Select and expand the group of Enforcers.

   The Enforcer group must include the LAN Enforcer for which you want to change the management server list.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Settings** dialog box, on the **General** tab, under **Communication**, select
     the management server list that you want this LAN Enforcer to use.

6   On the **General** tab, under **Communication**, click **Select**.

     You can view the IP addresses and host names of all available management
     servers, as well as the priorities that have been assigned to them.

7   In the **Management Server List** dialog box, click **Close**.

8   Click **OK**.

Using RADIUS server group settings

You can configure the LAN Enforcer to connect to one or more RADIUS servers.

You need to specify RADIUS servers as part of a RADIUS server group. Each group
can contain one or more RADIUS servers. The purpose of a RADIUS server group
is for RADIUS servers to provide failover. If one RADIUS server in the RADIUS
server group becomes unavailable, the LAN Enforcer tries to connect with another
RADIUS server that is part of the RADIUS server group.

You can add, edit, and delete the name of a RADIUS server group in the Symantec
Endpoint Protection Manager Console.

See "Adding a RADIUS server group name and RADIUS server" on page 926.

See "Editing the name of a RADIUS server group" on page 928.

See "Deleting the name of a RADIUS server group" on page 932.

Add, edit, and delete the name, host name, IP address, authentication port number,
and the shared secret of a RADIUS server in the Symantec Endpoint Protection
Manager Console.

See "Adding a RADIUS server group name and RADIUS server" on page 926.

See "Editing the friendly name of a RADIUS server" on page 929.

See "Editing the host name or IP address of a RADIUS server" on page 930.

See "Editing the authentication port number of a RADIUS server" on page 930.

See "Editing the shared secret of a RADIUS server" on page 931.

See "Deleting a RADIUS server" on page 933.

Adding a RADIUS server group name and RADIUS server

You can add a RADIUS server group name and RADIUS server at the same time.

To add a RADIUS server group name and RADIUS server

1   In the Symantec Endpoint Protection Manager, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **Add**.

    The name of the RADIUS server group and the IP address of an existing RADIUS server appear in the table.

6   In the **Add RADIUS Server Group** dialog box, type the name of the RADIUS server group in the **Group** text box.

    The name of the RADIUS server group, the host name or IP address of an existing RADIUS server, and the port number of the RADIUS server appear in the table.

7   Click **Add**.

8   In the **Add RADIUS Server** dialog box, type the following:

In the field: Friendly name of RADIUS server	Type a name that easily identifies the name of the RADIUS server when it appears on the list of servers for that group.
In the field: Hostname or IP address	Type the hostname or IP address of the RADIUS server.
In the field: Authentication port	Type the network port on the RADIUS server where the LAN Enforcer sends the authentication packet from the client. The default setting is 1812.
In the field: Switch timeout (in seconds)	Type the switch timeout value. The default is 3 seconds.
In the field: Switch retransmits	Type the switch retransmits value. The default is one.
In the field: Shared secret	Type the shared secret that is used for encrypted communication between the RADIUS server and the LAN Enforcer. The shared secret between a RADIUS server and a LAN Enforcer can be different from the shared secret between an 802.1x-aware switch and a LAN Enforcer. The shared secret is case sensitive.
In the field: Confirm shared secret	Type the shared secret again.

9   Click **OK**.

The name, Hostname or IP address, and port for the RADIUS server you added now appear in the **RADIUS Server Group** list in the **Add RADIUS Server Group** dialog box.

10   In the **Add RADIUS Server Group** dialog box, click **OK**.

11   In the **LAN Enforcer Settings** dialog box, click **OK**.

Editing the name of a RADIUS server group

You can change the name of the RADIUS server group at any time if circumstances change.

See "Using RADIUS server group settings" on page 926.

To edit the name of a RADIUS server group

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group of which the LAN Enforcer is a member.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab,
    click the RADIUS server group whose name you want to change.

6   Click **Edit**.

7   In the **Add RADIUS Server** dialog box, edit the name of the RADIUS server
    group in the **Group name** field.

8   Click **OK**.

9   In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab,
    click **OK**.

Editing the friendly name of a RADIUS server

You can change the friendly name of the RADIUS server at any time if
circumstances change.

See "Using RADIUS server group settings" on page 926.

To edit the friendly name of a RADIUS server

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group of which the LAN Enforcer is a member.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab,
    click the RADIUS server group that includes the RADIUS server whose friendly
    name you want to change.

6   Click **Edit**.

7   In the **Add a RADIUS Server** dialog box, edit the friendly name of the RADIUS
    server in the **Friendly name of RADIUS server** field.

8   Click **OK**.

9   In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab,
    click **OK**.

Editing the host name or IP address of a RADIUS server

You can change the host name or IP address of the RADIUS server at any time if circumstances change.

See "Using RADIUS server group settings" on page 926.

To edit the host name or IP address of a RADIUS server

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

3 Select the Enforcer group of which the LAN Enforcer is a member.

4 Under **Tasks**, click **Edit Group Properties**.

5 In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click the RADIUS server group that includes the RADIUS server whose host name or IP address you want to change.

6 Click **Edit**.

7 In the **Add a RADIUS Server** dialog box, edit the host name or IP address of the RADIUS server in the **Hostname or IP Address** field.

8 Click **OK**.

9 In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **OK**.

Editing the authentication port number of a RADIUS server

You can change the authentication port number of the RADIUS server at any time if circumstances change.

See "Using RADIUS server group settings" on page 926.

To edit the authentication port number of a RADIUS server

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

3 Select the Enforcer group of which the LAN Enforcer is a member.

4 Under **Tasks**, click **Edit Group Properties**.

5 In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click the RADIUS server group that includes the RADIUS server whose authentication port number you want to change.

6 Click **Edit**.

7   In the **Add a RADIUS Server** dialog box, edit the authentication port number
     of the RADIUS server in the **Authentication port** field.

8   Click **OK**.

9   In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab,
     click **OK**.

Editing the shared secret of a RADIUS server

You can change the shared secret of the RADIUS server at any time if
circumstances change.

See "Using RADIUS server group settings" on page 926.

To edit the shared secret of a RADIUS server

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group of which the LAN Enforcer is a member.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab,
     click the RADIUS server group that includes the RADIUS server whose shared
     secret you want to change.

6   In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab,
     click **Edit**.

7   In the **Add a RADIUS Server** dialog box, edit the shared secret of the RADIUS
     server in the **Shared secret** field.

     The shared secret is used for encrypted communication between the RADIUS
     server and the LAN Enforcer. The shared secret between a RADIUS server
     and a LAN Enforcer can be different from the shared secret between an
     802.1x-aware switch and a LAN Enforcer. The shared secret is case sensitive.

8   Edit the shared secret of the RADIUS server in the **Confirm shared secret**
     field.

9   Click **OK**.

10   In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab,
     click **OK**.

Enabling support for Windows Network Policy Server (NPS) on the LAN Enforcer

When you use a Microsoft Windows Server as a RADIUS server, it has in the past used Internet authentication server (IAS). With Windows Server 2008, IAS has been replaced with Network Policy Server (NPS). If you are using Server 2008, you must specify that you are using NPS.

Note: Enabling support for Windows NPS requires that clients and LAN Enforcers run Symantec Endpoint Protection version 11.0 RU6 MP2 or higher (including 12.1). If you enable this option on LAN Enforcers with legacy clients, Symantec Network Access Control functionality is not supported.

To enable support for Windows Network Policy Server

1 On the **Servers** screen, select the **LAN Enforcer**.

2 Under **Tasks**, click **Edit Group Properties**.

3 In the **LAN Enforcer Settings** dialog box, click the **RADIUS Server Group** tab.

4 At the bottom of the screen, click to **Enable support for Windows Network Policy Server (NPS)**.

   You will see a Warning note that is similar to the Note above. Be certain that your clients and LAN Enforcers are running version 11.0 RU6 MP2 or higher.

5 Click **OK** to save your configuration.

Deleting the name of a RADIUS server group

You can delete the name of the RADIUS server group at any time if circumstances change.

See "Using RADIUS server group settings" on page 926.

To delete the name of a RADIUS server group

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

3 Select the Enforcer group of which the LAN Enforcer is a member.

4 Under **Tasks**, click **Edit Group Properties**.

5 In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click the RADIUS server group whose name you want to delete.

6   Click **Remove**.

7   In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **OK**.

Deleting a RADIUS server

You can delete a RADIUS server at any time if circumstances change.

See "Using RADIUS server group settings" on page 926.

To delete a RADIUS server

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **Servers**, select the Enforcer group of which the LAN Enforcer is a member.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click the RADIUS server group of which the RADIUS server that you want to delete is a member.

6   In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **Edit**.

7   In the **Add RADIUS Server** dialog box, click the RADIUS server that you want to delete.

8   Click **Remove**.

9   Click **OK**.

10 In the **LAN Enforcer Settings** dialog box, on the **RADIUS Server Group** tab, click **OK**.

Using switch settings

You configure a switch policy when you specify LAN Enforcer settings for switches. A switch policy is a collection of settings that is applied to a group of switches of the same manufacturer or model. The only information that you need to enter separately for individual switches is the IP address of the switch.

See "Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard" on page 937.

See "Editing basic information about the switch policy and 802.1x-aware switch" on page 945.

Switch settings

You need to specify the following basic information before LAN Enforcer appliances, management servers, clients, and 802.1x-aware switches all work together:

- A name of your choice for the switch policy
- The switch manufacturer and model
  You select the switch model from a list of supported switches.
- The encrypted password or shared secret
- The RADIUS server group that is used
- The reauthentication timeout period for the 802.1x-aware switch
  The default setting is 30 seconds.
- Whether the switch forwards other protocols besides EAP
  The default setting is to forward other protocols.

See "Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard" on page 937.

See "Editing basic information about the switch policy and 802.1x-aware switch" on page 945.

You need to specify the following information for the set of 802.1x-aware switches to which the switch policy applies:

- A friendly switch name of your choice
- IP address, IP address range, or subnet

See "Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard" on page 937.

See "Editing information about the 802.1x-aware switch" on page 950.

You need to specify the following VLAN information:

- VLAN ID
- VLAN name
- Optionally, you can specify the customized RADIUS attributes in hexadecimal format.

See "Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard" on page 937.

See "Editing VLAN information for the switch policy" on page 951.

If an 802.1x-aware switch supports dynamic VLAN switching, you can specify that the client must connect to a specific VLAN.

You need to specify the actions that the 802.1x-aware switch needs to take when certain criteria are met:

■ Host authentication result: Pass, Fail, Unavailable, or Ignore Result

■ User authentication result: Pass, Fail, Unavailable, or Ignore Result

■ Policy Check result: Pass, Fail, Unavailable, or Ignore Result

See "Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard" on page 937.

About the support for attributes of switch models

When you configure the LAN Enforcer appliance, you specify the model of the 802.1x-aware switch. Different 802.1x-aware switches look for different attributes to determine which client can access the VLAN. Some switches identify VLANs by VLAN ID and others by VLAN Name. Some devices have limited or no VLAN support.

The LAN Enforcer appliance forwards attributes from the RADIUS server to the switch. If necessary, however, it modifies or appends the VLAN attribute based on the switch type by using supported values. If a conflict exists between the vendor-specific attribute information that the RADIUS server sends and the vendor-specific VLAN attribute information that the LAN Enforcer uses, the LAN Enforcer removes the vendor-specific information that the RADIUS server sends.

The LAN Enforcer then replaces that information with the information that appears in Table 49-1.

If you want to keep the attributes from the RADIUS server, you can select an action called **Open Port**. With this action, the LAN Enforcer forwards all attributes from the RADIUS server to the 802.1x-aware switch without any modifications.

The 802.1x-aware switch model can use VLAN ID or VLAN Name to perform dynamic VLAN assignments. Specify both the VLAN ID and VLAN name when you provide VLAN information for the LAN Enforcer, with the exception of the Aruba switch.

See "Changing LAN Enforcer configuration settings in Symantec Endpoint Protection Manager" on page 920.

Table 49-1 describes the 802.1x-aware switch models and attributes.

Table 49-1   Support for attributes of switch models

Switch model	Attributes added by LAN Enforcer	Comments
Airespace Wireless Controller	The vendor code is 14179. The vendor-assigned attribute number is 5. The attribute format is "string."	VLAN Name is used. Name is case sensitive.
Alcatel	Vendor Specific (#26) The vendor ID of Alcatel is 800. All "Vendor Specific" attributes from RADIUS with an ID of 800 are removed in case of conflict.	VLAN ID is used.
Aruba	Vendor Specific (#14823) Vendor ID is 14823 for Aruba. The Aruba-User-Role attribute permits you to set up either VLAN IDs or VLAN names.	Both VLAN name and VLAN ID can be used. Alternately, you can use only a VLAN name or only a VLAN ID. A valid VLAN ID ranges from 1 to 4094. A VLAN name cannot exceed 64 bytes.
Cisco Aironet Series	Depends on whether you use SSID access control. RADIUS user attributes used for VLAN-ID assignment: IETF 64 (Tunnel Type): Set this attribute to "VLAN" IETF 65 (Tunnel Medium Type): Set this attribute to "802" IETF 81 (Tunnel Private Group ID): Set this attribute to VLAN-ID RADIUS user attribute used for SSID access control: Cisco IOS/PIX RADIUS Attribute, 009\001 cisco-av-pair	VLAN ID is used.
Cisco Catalyst Series	Tunnel Type (#64) Tunnel Medium Type (#65) Tunnel Private Group ID (#81) Tunnel Type is set to 13 (VLAN) Tunnel Medium Type is set to 6 (802 media) Tunnel Private Group ID is set to VLAN name. All attributes with these three types from RADIUS server are removed in case of conflict. Also, any attribute with type "Vendor Specific" and the vendor ID is 9 (Cisco) are also removed.	VLAN Name is used. Name is case sensitive.

Table 49-1	Support for attributes of switch models *(continued)*	
Switch model	**Attributes added by LAN Enforcer**	**Comments**
Foundry, HP, Nortel, 3com, Huawei	Tunnel Type (#64) Tunnel Medium Type (#65) Tunnel Private Group ID (#81) Tunnel Type is set to 13 (VLAN) Tunnel Medium Type is set to 6 (802 media) Tunnel Private Group ID is set to VLAN ID. All attributes with these three types from RADIUS server are removed in case of conflict.	VLAN ID is used.

Enterasys	Filter ID (#11)
	
	Filter ID is set to
	
	`Enterasys :`
	
	`version=1:`
	
	`mgmt=su:`
	
	`policy=NAME`
	
	All "Filter ID" attributes from RADIUS Server are removed in case of conflict.
		VLAN Name is used and represents "Role name" in the Enterasys switch. The name is case sensitive.

Extreme	Vendor Specific (#26) Vendor ID is 1916 for Extreme. VLAN Name is added after the Vendor ID. All vendor-specific attributes from RADIUS server with an ID of 1916 are removed in case of conflict.	VLAN Name is used. The name is case sensitive.

Adding an 802.1x switch policy for a LAN Enforcer appliance with a wizard

You can add multiple 802.1x-aware switches for use with a LAN Enforcer appliance as part of a switch policy. You must enter the information that is needed to configure the LAN Enforcer appliance interaction with the switch.

See "Using switch settings" on page 933.

To add an 802.1x switch policy for a LAN Enforcer appliance with a wizard

1   In Symantec Endpoint Protection Manager, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **Add**.

6   In the **Welcome to the Switch Policy Configuration Wizard** panel of the **Switch Policy Configuration Wizard,** click **Next**.

7   In the **Basic Information** panel of the **Switch Policy Configuration Wizard**, complete the following tasks:

Switch policy name	Type a name of your choice that identifies the switch policy.
	For example, you can use the manufacturer's name and model as the name for the switch policy name.

Switch model	The LAN Enforcer uses the switch model to determine the vendor-specific RADIUS server attribute.
	Select one of the following 802.1x-aware models from the list of supported switches:

- Other
  If your model is not listed, select **Other** to use a generic RADIUS server attribute.
- 3Com
- Alcatel switch
- Cisco Catalyst Series
- Enterasys Matix Series
- Extreme Summit Series
- Foundry Networks
- HP Procure Series
- Nortel BayStack Series
- Cisco Aironet Series
- Aruba Switches
- Airespace Wireless Controller
- Nortel Wireless
- Enterasys wireless controller
- Allied Telesis switches
- HuaWei switches later than Jan. 2009

  Note: For the HuaWei switches, If the administrator chooses transparent mode on the switch, the administrator must configure the policy to use transparent mode on the client, rather than letting the user select it.

Shared secret	The shared secret that is used for communication between the 802.1x-aware switch and the LAN Enforcer appliance. The shared secret is case sensitive.
Confirm shared secret	You must type the shared secret again.
RADIUS server group	If you use the LAN Enforcer appliance with a RADIUS server, you must select the RADIUS server group from the available RADIUS server group list.

Reauthentication period (seconds)	Type the amount of time in seconds during which the client must be reauthenticated. Otherwise the client is removed from the list of connected clients on the LAN Enforcer.
	You should set the reauthentication period to be at least double the amount of time of the reauthentication interval on the switch.
	For example, if the reauthentication interval on the switch is 30 seconds, the LAN Enforcer appliance reauthentication period should be at least 60 seconds. Otherwise the LAN Enforcer appliance assumes that the client is timed out. Therefore the client does not release and renew its IP address.
	The default setting is 30 seconds.
Forward protocols besides EAP	You can select this option to allow the LAN Enforcer appliance to forward the RADIUS packets that contain other authentication protocols besides EAP. Other protocols include Challenge Handshake Authentication Protocol (CHAP) and PAP.
	The default setting is enabled.

8 In the **Basic Information** panel of the **Switch Policy Configuration Wizard**, click **Next**.

9 In the **Switch List** panel of the **Switch Policy Configuration Wizard**, click **Add**.

10 Complete the following tasks:

Name	In the **Add Single Internal IP address** dialog box, type a friendly name for the switch policy to identify the 802.1x-aware switch into the Name field.
Single IP Address	In the **Add Single Internal IP Address** dialog box, click **Single IP address**. Then type the IP address of the 802.1x-aware switch in th**e IP Address** field.
IP Address Range	In the **Add Internal IP Address Range** dialog box, click **IP Address Range**. Type the beginning IP address for the 802.1x-aware switch in the **Starting IP Address** field. Type the ending IP address of the IP address range for the 802.1x-aware switch in the **End IP** field.
Subnet	In the **Add Internal IP Address Subnet** dialog box, click **Subnet**. Type the IP address for the subnet in the **IP address** field and the subnet in the **Subnet Mask** field.

When you specify a switch policy for a LAN Enforcer appliance, you can associate the switch policy with one or more 802.1x-aware switches.

11 In the **Add Internal IP address** dialog box, click **OK**.

12 In the **Switch List** panel of the **Switch Policy Configuration Wizard**, click **Next**.

13 In the **Switch VLAN Configuration** panel of the **Switch Policy Configuration Wizard**, click **Add**.

14 In the **Add VLAN** dialog box, complete the following tasks:

VLAN ID	Type an integer that can range from 1 to 4094 in the VLAN ID field.
	The VLAN ID must be the same as the one that is configured on the 802.1x-aware switch except for the Aruba switch.
	If you plan to add VLAN information about an Aruba switch, you may want to configure VLAN and role information differently than you have for other 802.1x switches.
	See "Configuring VLAN and role information on the 802.1x-aware Aruba switch" on page 953.
VLAN Name	Type a name of the VLAN.
	The name for the VLAN can be up to 64 characters. It is case sensitive.
	The VLAN name must be the same as the one that is configured on the 802.1x-aware switch except for the Aruba switch.
	If you plan to add VLAN information about an Aruba switch, you may want to configure VLAN and role information that is different from other 802.1x switches.
	See "Configuring VLAN and role information on the 802.1x-aware Aruba switch" on page 953.
Send customized RADIUS attributes to switch	Check **Send customized RADIUS attributes to switch** if you want the LAN Enforcer to send a customized RADIUS attribute to the 802.1x-aware switch. An attribute can be an access control list (ACL).
	See "About the support for attributes of switch models" on page 935.
Customized attributes in hex format	Type the RADIUS attribute in hex format.
	The length must be even.

When you specify a switch policy for a LAN Enforcer, you use the **VLAN** tab to add the VLAN information for each VLAN that is configured on the switch. You want the switch policy to be available for use by the LAN Enforcer as an action. The best practice is to specify at least one remediation VLAN.

15 Click **OK**.

16 In the **Switch VLAN Configuration** panel of the **Switch Policy Configuration Wizard**, click **Next**.

17 In the **Switch Action Configuration** panel of the **Switch Policy Configuration Wizard**, click **Add**.

18 In the **Add Switch Action** dialog box, complete the following tasks:

Host Authentication   Click any of the following conditions:

- Passed
- Failed
- Unavailable
- Ignore Result

A typical situation in which a Host Integrity check becomes unavailable would be the result of a client not running. If you set Host Authentication to Unavailable, you must also set Policy Check to Unavailable.

User Authentication   Click any of the following conditions:

- Passed
  The client has passed user authentication.
- Failed
  The client has not passed user authentication.
- Unavailable
  The user authentication result is always unavailable if user authentication is not performed in transparent mode. If you use the LAN Enforcer in transparent mode, you must create an action for the Unavailable condition.
  If you use the basic configuration, you may also want to configure an action for the user authentication as an error condition. For example, an 802.1x supplicant uses an incorrect user authentication method or the RADIUS server fails in the middle of the authentication transaction.
  The user authentication's Unavailable condition may also occur on some RADIUS servers if the user name does not exist in the RADIUS database. For example, this problem may occur with Microsoft IAS. Therefore you may want to test the condition of a missing user name with your RADIUS server. You may want to see whether it matches the Failed or Unavailable user authentication conditions.
- Ignore Result

A typical situation in which a Host Integrity check becomes unavailable would be the result of a client not running. If you set Policy Check to Unavailable, you must also set Host Authentication to Unavailable.

Policy Check	Click any of the following conditions:

- Passed
  The client has passed the Policy Check.
- Failed
  The client has not passed the Policy Check.
- Unavailable
  The Unavailable result for the policy may occur under the following conditions:
  - If the client has an invalid identifier, then the LAN Enforcer cannot obtain any policy information from the management server. This problem can occur if the management server that deployed the client policy is no longer available.
  - If the client is first exported and installed before it connects to the management server and receives its policy.
- Ignore Result

Action	You can select the following actions that the 802.1x-aware switch performs when the conditions are met:

- Open Port
  The 802.1x-aware switch allows network access on the default VLAN to which the port is normally assigned. It also allows network access on the VLAN that is specified in an attribute that is sent from the RADIUS server. Therefore the support of users having VLAN access is based on user ID and user role.
  The default action is Open Port.
- Switch to VLAN-*test*
  Allows access to the specified VLAN. The VLANs that are available to select are the ones that you configured previously.
- Close Port
  Deny network access on the default or RADIUS-specified VLAN. On some switch models, depending on the switch configuration, the port is assigned to a guest VLAN.

For the Aruba switch, you can restrict access according to a specified role as well as a specified VLAN. The restrictions depend on how you configured the VLAN information for the switch policy.

19 In the **Add Switch Action** dialog box, click **OK**.

20 In the **Switch Action Configuration** panel of the **Switch Policy Configuration Wizard**, in the **Switch Action** table, click the switch action policy whose priority you want to change.

The LAN Enforcer checks the authentication results against the entries in the switch action table in the order from top to bottom of the table. After it finds a matching set of conditions, it instructs the 802.1x-aware switch to apply that action. You can change the sequence in which actions are applied by changing the order in which they are listed in the table.

21 Click **Move Up** or **Move Down**.

22 Click **Next**.

23 In the **Complete the Switch Policy Configuration** panel of the **Switch Policy Configuration Wizard**, click **Finish**.

Editing basic information about the switch policy and 802.1x-aware switch

You can change the following parameters about the switch policy and the 802.1x-aware switch:

- Switch policy name
  See "Editing the name of a switch policy" on page 945.

- Switch model
  See "Selecting a different switch model for the switch policy" on page 946.

- Shared secret
  See "Editing an encrypted password or shared secret" on page 947.

- RADIUS server group
  See "Selecting a different RADIUS server group" on page 948.

- Reauthentication time period
  See "Editing the reauthentication period" on page 948.

- Forwarding protocols besides EAP
  See "Enabling protocols other than EAP" on page 949.

Editing the name of a switch policy

You can edit the name of the switch policy at any time if circumstances change.

See "Switch settings" on page 934.

To edit the name of a switch policy

1   In Symantec Endpoint Protection Manager, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy that you want to change.

6   Click **Edit**.

7   In the **Edit Switch Policy for** *name of switch policy* dialog box, on the **Basic Information** tab, edit the name of the switch policy in the **Switch policy name** field.

8   Click **OK**.

9   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Selecting a different switch model for the switch policy

You can select a different switch model for the switch policy at any time if circumstances change.

See "Switch settings" on page 934.

To select a different switch model for the switch policy

1   In Symantec Endpoint Protection Manager, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose switch mode you want to change.

6   Click **Edit**.

7   In the **Edit Switch Policy for** *name of switch policy* dialog box, on the **Basic Information** tab, select a different switch model from the following Switch model list:

   ■ Other
      If your model is not listed, select **Other** to use a generic RADIUS server attribute.

   ■ 3Com

- Alcatel switch

- Cisco Catalyst Series

- Enterasys Matix Series

- Extreme Summit Series

- Foundry Networks

- HP Procurve Series

- Nortel BayStack Series

- Cisco Aironet Series

- Aruba Switches

- Airespace Wireless Controller

- Nortel Wireless

- Enterasys wireless controller

- HuaWei switch
  If the administrator chooses transparent mode on the HuaWei switch, the
  administrator must configure the policy to use transparent mode on the
  client, rather than letting the user select it.

8   Click **OK**.

9   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Editing an encrypted password or shared secret

You can edit the shared secret at any time if circumstances change.

To edit an encrypted password or shared secret

1   In Symantec Endpoint Protection Manager, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose shared secret you want to change.

6   Click **Edit**.

7   In the **Edit Switch Policy for** *name of switch policy* dialog box, on the **Basic Information** tab, edit the name of the shared secret in the **Shared secret** field.

8   Edit the name of the shared secret in the **Confirm shared secret** field.

9   Click **OK**.

10 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Selecting a different RADIUS server group

You can select a different RADIUS server group at any time if circumstances change.

See "Switch settings" on page 934.

To select a different RADIUS server group

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose shared secret you want to change.

6   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click **Edit**.

7   In the **Edit Switch Policy for** *name of switch policy* dialog box, on the **Basic Information** tab, select a different RADIUS server group from the RADIUS server group list.

    You must have added more than one RADIUS server group before you can select a different RADIUS server group.

8   Click **OK**.

9   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Editing the reauthentication period

You can edit the reauthentication period at any time if circumstances change.

You must specify the amount of time in seconds during which the client must be reauthenticated. Otherwise the client is removed from the list of connected clients and disconnected from the network.

You should set the reauthentication period to be at least double the amount of time of the reauthentication interval on the switch.

For example, if the reauthentication interval on the switch is 30 seconds, the LAN Enforcer reauthentication period should be at least 60 seconds. Otherwise the

LAN Enforcer assumes that the client is timed out. Therefore the client does not release and renew its IP address.

The default setting is 30 seconds.

See "Switch settings" on page 934.

To edit the reauthentication period

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group.

4   Click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy that you want to change.

6   Click **Edit**.

7   In the **Edit Switch Policy for *name of switch policy*** dialog box, on the **Basic Information** tab, edit the reauthentication period in the Reauthentication period in seconds field.

8   Click **OK**.

9   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Enabling protocols other than EAP

You can make the selections that allow the LAN Enforcer to forward the RADIUS packets that contain other authentication protocols besides EAP.

Other protocols include:

■   Challenge Handshake Authentication Protocol (CHAP)

■   PAP

The default setting is enabled.

See "Switch settings" on page 934.

To enable protocols other than EAP

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group.

4   Click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy that you want to change.

6   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the Switch
    Policy table, click **Edit**.

7   In the **Edit Switch Policy for** *name of switch policy* dialog box, on the **Basic
    Information** tab, check **Enable protocols besides EAP**.

    You can have the following protocols forwarded:

    ■   Challenge Handshake Authentication Protocol (CHAP)

    ■   PAP

8   Click **OK**.

9   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Editing information about the 802.1x-aware switch

You can change the following parameters about the 802.1x-aware switch:

■   Change of IP address, host name, or subnet for an 802.1x-aware switch
    See "Editing the IP address, host name, or subnet of an 802.1x-aware switch"
    on page 950.

■   Removal of an 802.1x-aware switch from switch list
    See "Deleting an 802.1x-aware switch from the switch list" on page 951.

Editing the IP address, host name, or subnet of an 802.1x-aware switch

You can change the IP address, hostname, or subnet of an 802.1x-aware switch
at any time if circumstances require it.

See "About the support for attributes of switch models" on page 935.

To edit the IP address, hostname, and subnet of an 802.1x-aware switch

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch
    Policy** table, click the switch policy that you want to change.

6   Click **Edit**.

7   In the **Edit Switch Policy for** *name of switch policy* dialog box, on the **Switch
    Address** tab, check **Edit All**.

8   In the **Edit IP Addresses** dialog box, add or edit IP addresses, host, names, or subnets for the 802.1x-aware switch.

The format of the text is as follows:

Single IP Address	*name*: *address*
IP address range	*name*: *start address-end address*
Subnet	*name*: *start address/subnet mask*

9   Click **OK**.

10 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Deleting an 802.1x-aware switch from the switch list

You can delete an 802.1x-aware switch from the switch list at any time if circumstances require it.

See "About the support for attributes of switch models" on page 935.

To delete an 802.1x-aware switch

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the 802.1x-aware switch that you want to delete from the switch list.

6   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **Remove**.

7   Click **OK**.

Editing VLAN information for the switch policy

You can change the following parameters about VLANs on the 802.1x-aware switch:

■ Change the VLAN ID and VLAN name of an 802.1x-aware switch
See "Editing the VLAN ID and VLAN name of an 802.1x-aware switch" on page 952.

■ Configure VLAN and role information on the 802.1x-aware Aruba switch

See

■ Removal of VLANs on an 802.1x-aware switch

Editing the VLAN ID and VLAN name of an 802.1x-aware switch

You can change the VLAN ID and VLAN name of an 802.1x-aware switch at any time if circumstances require it.

Some switches, such as the Cisco switch, have a guest VLAN feature. The guest VLAN is normally used if EAP user authentication fails. If EAP authentication fails, the switch connects the client to the guest VLAN automatically.

If you use the LAN Enforcer for VLAN switching, it is recommended that you do not use the reserved guest VLAN when you set up VLANs and actions on the LAN Enforcer. Otherwise the 802.1x supplicant may respond as if EAP authentication failed.

When setting up VLANs, make sure that all of them can communicate with the management server.

See

To edit the VLAN ID and VLAN name of an 802.1x-aware switch

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose VLAN information you want to change.

6   Click **Edit**.

7   In the **Edit Switch Policy for** *name of switch policy* dialog box, on the **Switch Address** tab, select the VLAN that you want to edit.

8   On the **VLAN** tab, check **Edit**.

9   In the **Edit VLAN** dialog box, edit the VLAN ID in the **VLAN ID** field.

10   Edit the VLAN name in the **VLAN name** field.

If you plan to edit VLAN information about an Aruba switch, you may want to configure VLAN and role information somewhat differently than you have for other 802.1x switches.

See "Configuring VLAN and role information on the 802.1x-aware Aruba switch" on page 953.

11   In the **Edit Switch Policy for** *name of switch policy* dialog box, on the **VLAN** tab, click **OK**.

12   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Deleting the VLANs on an 802.1x-aware switch

You can delete the VLANs on an 802.1x-aware switch at any time if circumstances require it.

See "Switch settings" on page 934.

To delete the VLANs on an 802.1x-aware switch

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   click **Servers**.

3   Select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose VLAN information you want to delete.

6   Click **Edit**.

7   In the **Edit Switch Policy for** *name of switch policy* dialog box, on the **Switch Address** tab, select the VLAN that you want to delete.

8   On the **VLAN** tab, check **Remove**.

9   Click **OK**.

10   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Configuring VLAN and role information on the 802.1x-aware Aruba switch

If you use an Aruba switch, you can leave the VLAN ID or the VLAN name field blank. However, for other switches, you must enter information in both fields. For the Aruba switch, you can use these fields to specify either a VLAN or a role or both as follows:

■ To specify a VLAN, enter the VLAN ID in the VLAN ID field.

■ To specify a role, enter the role name in the VLAN name field.

For the Aruba switch you can also use this dialog box to set up separate switch actions for multiple roles on one VLAN or multiple VLANS for one role.

See "Switch settings" on page 934.

To configure VLAN and role information on the 802.1x-aware Aruba switch

1 If you had a VLAN ID 1 with role A and role B, fill in the VLAN ID as 1 and the VLAN name as A. Click **OK**.

2 Click **Add** again. In the **Add VLAN** dialog box, fill in the VLAN ID as 1 and the VLAN name as B and click **OK**.

Two separate choices become available for configuration on the switch action table.

Editing action information for the switch policy

You can change the following parameters about VLANs on the 802.1x-aware switch:

■ Set the order of condition checking
See "Setting the order of condition checking" on page 955.

■ Select a different Host Authentication, User Authentication, or Policy Check condition
See "Selecting a different Host Authentication, User Authentication, or Policy Check condition" on page 956.

■ Select different actions
See "Selecting different actions" on page 957.

About issues with the switch policy, associated conditions, and actions

When configuring switch policies, note the following:

■ The Switch Action table must contain at least one entry.

■ If you do not select an action for a particular combination of results, the default action, Open Port, is performed.

■ To specify a default action for any possible combination of results, select Ignore Result for all three results.

■ When you add the actions to the table, you can edit any cell by clicking on the right corner of a column and row to display a drop-down list.

- Some switches, such as the Cisco switch, have a guest VLAN feature. The guest VLAN is normally intended to be used if user authentication fails. In other words, if user authentication fails, the switch connects the client to the guest VLAN automatically.

  If you use the LAN Enforcer for VLAN switching, it is recommended that you do not use the reserved guest VLAN when setting up VLANs and actions on the LAN Enforcer. Otherwise the 802.1x supplicant may respond as though user authentication failed.

- If you deploy clients and are not ready to implement the full capabilities of the LAN Enforcer, you can specify an action of allowing access to the internal network that is based on the condition Ignore Result for the Host Integrity check and Policy Check. If you want to disregard the user authentication results and allow network access regardless of the results, you can do so with the condition Ignore Result for User Authentication results.

See "Setting the order of condition checking" on page 955.

See "Selecting a different Host Authentication, User Authentication, or Policy Check condition" on page 956.

See "Selecting different actions" on page 957.

Setting the order of condition checking

You can change a different Host Authentication, User Authentication, or Policy Check condition for a switch policy at any time if circumstances require it.

You can add an entry to the Switch Action table for each of the possible combinations of authentication results.

When you set up the conditions to check for, remember that the only circumstance in which all three results can be Pass or Fail is in the basic configuration. In the basic configuration, the client runs both an 802.1x supplicant that provides information about user authentication and a client that provides information about Host Integrity and the Policy Serial Number.

If you run only an 802.1x supplicant without a client, the results for the Host Integrity check and Policy Check are always unavailable. If you run in transparent mode without a user authentication check, the user authentication result is always Unavailable.

The LAN Enforcer checks the authentication results against the entries in the table in the order from top to bottom of the table. After the LAN Enforcer finds a matching set of conditions, it instructs the 802.1x-aware switch to apply that action. You can change the sequence in which actions are applied by changing the order in which they are listed in the table.

If a LAN Enforcer cannot locate any entry that matches the current condition, a CLOSE PORT action is taken.

See "About issues with the switch policy, associated conditions, and actions" on page 954.

To set the order of condition checking

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   In the Admin page, click **Servers**.

3   Select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose order of conditions checking you want to change.

6   Click **Edit**.

7   In the **Edit Switch Policy for** *name of switch policy* dialog box, on the **Action** tab, select the switch policy whose order of conditions checking you want to change.

8   Click **Move Up** or **Move Down**.

9   Click **OK**.

10 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Selecting a different Host Authentication, User Authentication, or Policy Check condition

You can select a different Host Authentication, User Authentication, or Policy Check condition for a switch policy at any time if circumstances require it.

See "About issues with the switch policy, associated conditions, and actions" on page 954.

To select a different Host Authentication, User Authentication, or Policy Check condition

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose authentication conditions you want to change.

6   Click **Edit**.

7   In the **Edit Switch Policy for** *name of switch policy* dialog box, on the **Action** tab, click any of the authentication conditions that you want to change in any of the following columns:

   ■ Host authentication

   ■ User authentication

   ■ Policy check

8   Select any of the following actions that the 802.1x-aware switch needs to take when certain criteria are met:

   ■ Host authentication result: Pass, Fail, Unavailable, or Ignore Result

   ■ User authentication result: Pass, Fail, Unavailable, or Ignore Result

   ■ Policy Check result: Pass, Fail, Unavailable, or Ignore Result

9   Click **OK**.

10 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Selecting different actions

You can select the different actions that the 802.1x-aware switch can take when certain criteria are met:

See "About issues with the switch policy, associated conditions, and actions" on page 954.

To select a different Host Authentication, User Authentication, or Policy Check condition

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select the Enforcer group.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **LAN Enforcer Settings** dialog box, on the **Switch** tab in the **Switch Policy** table, click the switch policy whose actions you want to change.

6   Click **Edit**.

7 On the **Action** tab, click any of the actions that you want to change in the **Action** column.

8 Select any of the following actions that the 802.1x-aware switch needs to take when certain criteria are met:

- Open Port
  The 802.1x-aware switch allows network access on the default VLAN to which the port is normally assigned. It also allows network access on the VLAN that is specified in an attribute that is sent from the RADIUS server. Therefore the support of users having VLAN access is based on user ID and user role.
  The default action is Open Port.

- Switch to VLAN-*test*
  Allows access to the specified VLAN. The VLANs that are available to select are the ones that you configured previously.

- Close Port
  Deny network access on the default or RADIUS-specified VLAN. On some switch models, depending on the switch configuration, the port is assigned to a guest VLAN.

9 Click **OK**.

10 In the **LAN Enforcer Settings** dialog box, on the **Switch** tab, click **OK**.

Using advanced LAN Enforcer appliance settings

You can configure the following advanced LAN Enforcer appliance configuration settings:

- Allow a legacy client.
  See "Allowing a legacy client to connect to the network with a LAN Enforcer appliance" on page 959.

- Enable local authentication.
  See "Enabling local authentication on the LAN Enforcer appliance" on page 959.

- Add/Edit/Remove/Import/Export MAC address and associated VLAN for MAC Authentication Bypass.
  See "Configuring MAC addresses and MAC authentication bypass (MAB) on the LAN Enforcer" on page 960.

- Enabling Network Time Protocol, and the server that provides the service.

- Enabling management server health check and interval period.

Details on implementing each of these settings appear on the context-sensitive help page for LAN Enforcer appliance advanced settings.

Allowing a legacy client to connect to the network with a LAN Enforcer appliance

You can enable a LAN Enforcer appliance to connect to 5.1.x legacy clients. If your network supports an 11.0.2 Symantec Endpoint Protection Manager, a Symantec LAN Enforcer appliance, and needs to support 5.1.x legacy clients, you can enable the support of 5.1.x legacy clients on the management server console so that the Symantec LAN Enforcer appliance does not block them.

See "Using advanced LAN Enforcer appliance settings" on page 958.

To allow a legacy client to connect to the network with a LAN Enforcer appliance

1   In Symantec Endpoint Protection Manager, click **Admin**.

2   Click **Servers**.

3   Select and expand the group of LAN Enforcers appliances.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Settings** dialog box, on the **Advanced** tab, check **Allow legacy clients**.

6   Click **OK**.

Enabling local authentication on the LAN Enforcer appliance

If a LAN Enforcer appliance loses its connection with the computer on which the Symantec Endpoint Protection Manager is installed, the LAN Enforcer appliance can authenticate a client locally.

See "Using advanced LAN Enforcer appliance settings" on page 958.

To enable local authentication on the LAN Enforcer appliance

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the group of LAN Enforcer appliances.

4   Select the LAN Enforcer appliance group for which you want to enable local authentication.

5   Under **Tasks**, click **Edit Group Properties**.

6   In the **LAN Settings** dialog box, on the **Advanced** tab, check **Enable Local Authentication**.

7   Click **OK**.

Enabling system time updates for the Enforcer appliance using the Network Time Protocol

With Network Time Protocol (NTP) enabled, Enforcer appliance clocks can update to the correct time. This setting is disabled by default, but it can be overridden if it is specified in a group policy.

See "Using advanced LAN Enforcer appliance settings" on page 958.

To enable time updates for the LAN Enforcer appliance from the Symantec Endpoint Protection Manager

1   In the Symantec Endpoint Protection Manager, click **Admin**.

2   Click **Servers**.

3   Under **Servers**, select and expand the group of LAN Enforcer appliances.

4   Under **Tasks**, click **Edit Group Properties**.

5   On the **Advanced** tab, check **Enable Network Time Protocol**.

6   Enter the IP address or the fully qualified domain name of the NTP server.

7   Click **OK**.

From the Enforcer console, you can temporarily change this setting to help troubleshoot time synchronization issues. From the Enforcer console command line, enter

`Enforcer (configure)` **# ntp**.

Note: If you had enabled NTP in an earlier version of Symantec Endpoint Protection, that configuration is lost when you upgrade. You must re-enable NTP.

Configuring MAC addresses and MAC authentication bypass (MAB) on the LAN Enforcer

You can change the MAC authentication settings on a management server. The configuration settings are automatically downloaded from the management server to the LAN Enforcer appliance during the next heartbeat.

To configure MAC addresses and MAC authentication bypass on the LAN Enforcer

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **Servers**, select and expand the group of Enforcers.

4   Select the LAN Enforcer.

5   Under **Tasks**, click **Edit Group Properties**.

6   Open the **Advanced** tab.

7   In the dropdown list on the left, select **MAC Authentication Bypass**, and click **Enable**.

8   In the **Settings** dialog box, on the **Advanced** tab, next to **MAC address**, click **Add**.

9   In the **Add Trusted Host** dialog box, type the MAC address for the client or the trusted host in the Host MAC address field.

   When you specify a MAC address, you can use a wildcard character if you type it for all three fields on the right.

   For example, 11-22-23-*-*-* represents the correct use of the wildcard character. However, 11-22-33-44-*-66 does not represent the correct use of the wildcard character.

   You can also copy a set of MAC addresses from a text file.

   Note: Symantec supports the following format for imports: single MAC address, and MAC address with mask.

   To import MAC addresses, click **Import**. Specify the file in the **Import MAC Address From File** dialog box.

   To export MAC addresses, highlight several MAC addresses, and then click **Export**. Specify the file in the **Export MAC Address To File** dialog box.

10 Click **OK**.

Using 802.1x authentication

If your corporate network uses a LAN Enforcer for authentication, you must configure the client computer to perform IEEE 802.1x authentication.

The 802.1x authentication process includes the following steps:

■   An unauthenticated client or third-party supplicant sends the user information and compliance information to a managed 802.11 network switch.

■   The network switch relays the information to the LAN Enforcer appliance. The LAN Enforcer appliance sends the user information to the authentication server for authentication. The RADIUS server is the authentication server.

■ If the client fails the user-level authentication or is not in compliance with the Host Integrity policy, the Enforcer may block network access. The LAN Enforcer appliance places the non-compliant client computer in network according to the Switch Action table where the computer can be remediated.

■ After the client remediates the computer and brings it into compliance, the 802.1x protocol reauthenticates the computer and grants the computer access to the network.

To work with the LAN Enforcer appliance, the client can use either a third-party supplicant or a built-in supplicant.

Table 49-2 describes the types of options that you can configure for 802.1x authentication.

Table 49-2   802.1x authentication options

Option	Description
Third-party supplicant	Uses a third-party 802.1x supplicant.
	The LAN Enforcer appliance works with a RADIUS server and third-party 802.1x supplicants to perform user authentication. The 802.1x supplicant prompts users for user information, which the LAN Enforcer passes to the RADIUS server for user-level authentication. The client sends the client profile and the Host Integrity status to the LAN Enforcer appliance so that it authenticates the computer.
	Note: If you want to use the Symantec Network Access Control client with a third-party supplicant, then you must install the Network Threat Protection module of the Symantec Network Access Control client.
	To use a third-party 802.1x supplicant, you must:
	■ Configure the 802.1x switch to use the LAN Enforcer appliance as the RADIUS server so that the switch forwards authentication packets to the LAN Enforcer appliance.
	■ Add the LAN Enforcer appliance as a client of the RADIUS server so that it accepts requests from the LAN Enforcer appliance.
	■ In the console, you must specify the RADIUS server information and enable 802.1x authentication for the clients.

Table 49-2   802.1x authentication options *(continued)*

Option	Description
Transparent mode	Uses the client to run as an 802.1x supplicant.
	You use this method if you do not want to use a RADIUS server to perform user authentication. The LAN Enforcer appliance runs in transparent mode and acts as a pseudo-RADIUS server.
	Transparent mode means that the supplicant does not prompt users for user information. In transparent mode, the client acts as the 802.1x supplicant. The client responds to the switch's EAP challenge with the client profile and the Host Integrity status. The switch, in turn, forwards the information to the LAN Enforcer appliance, which acts as a pseudo-RADIUS server. The LAN Enforcer appliance validates the Host Integrity and client profile information from the switch and can allow, block, or dynamically assign a VLAN, as appropriate.
	Note: To use a client as an 802.1x supplicant, you must uninstall or disable third-party 802.1x supplicants on the client computer.
	In transparent mode, you can leave the RADIUS server information empty on the LAN Enforcer Settings dialog box. The RADIUS server IP address is therefore set to 0 and no traditional EAP user authentication takes place.
Built-in supplicant	Uses the client computer's built-in 802.1x supplicant.
	The built-in authentication protocols include Smart Card, PEAP, or TLS. After you enable 802.1x authentication, you or the users must specify which authentication protocol to use.

Warning: You must know whether your corporate network uses the RADIUS server as the authentication server. If you configure 802.1x authentication incorrectly, the connection to the network may break.

Note: To enable the user to configure 802.1x authentication on the client, you must set the client to client control.

See "How the LAN Enforcer appliance works" on page 788.

To configure the client to use either transparent mode or a built-in supplicant

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

2   Under **View Client**s, select the group of the clients that you want to perform 802.1x authentication.

3   On the **Policies** tab, under **Settings**, click **General Settings**.

4   On the **Security Settings** tab, check **Enable 802.1x authentication**.

5   Check **Use the client as an 802.1x supplicant**.

6   Do one of the following actions:

   ■ To select transparent mode, select **Use Symantec Transparent Mode**.

   ■ To enable the user to configure a built-in supplicant, select **Allows user
      to select the authentication protocol**.
      Users can choose the authentication protocol for their network connection.

7   Click **OK**.

To configure the client to use a third-party supplicant

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

2   Under **View Clients**, select the group of the clients that you want to perform
    802.1x authentication.

3   On the **Policies** tab, under **Settings**, click **General Settings**.

4   On the **Security Settings** tab, check **Enable 802.1x authentication**.

5   Click **OK**.

    You can configure the client to use the built-in supplicant. You enable the
    client for both 802.1x authentication and as an 802.1x supplicant.

About reauthentication on the client computer

If the client computer passed the Host Integrity check but the Enforcer blocks the
computer, users may need to reauthenticate their computers. Under normal
circumstances, users should never need to reauthenticate the computer.

The Enforcer may block the computer when one of the following events has
occurred:

■ The client computer failed the user authentication because users typed their
   user name or their password incorrectly.

■ The client computer is in the wrong VLAN.

■ The client computer does not obtain a network connection. A broken network
   connection usually happens because the switch between the client computer
   and the LAN Enforcer did not authenticate the user name and password.

■ Users need to log on to a client computer that authenticated a previous user.

■ The client computer failed the compliance check.

Users can reauthenticate the computer only if you configured the computer with a built-in supplicant. The right-click menu on the notification area icon of the client computer displays a Reauthentication command.

See "Using 802.1x authentication" on page 961.

Managing Enforcers on the Symantec Endpoint Protection Manager

This chapter includes the following topics:

- About managing Enforcers on the management server console
- About managing Enforcers from the Servers page
- About Enforcer groups
- About the Enforcer information that appears on the Enforcer console
- Displaying information about the Enforcer on the management console
- Changing an Enforcer's name and description
- Deleting an Enforcer or an Enforcer group
- Exporting and importing Enforcer group settings
- Pop-up messages for blocked clients
- About client settings and the Enforcer
- Configuring clients to use a password to stop the client service
- About Enforcer reports and logs
- Configuring Enforcer log settings

About managing Enforcers on the management server console

The Symantec Enforcer settings on the management server console help you configure the Enforcer, its authentication interactions, and enforcement interactions with clients. Before you configure the Enforcer settings on the console, you complete the installation and setup of the Enforcer on the Enforcer appliance or computer.

The Enforcer settings on the Symantec Endpoint Protection Manager console depend on which type of Enforcer appliance you configure: Gateway or LAN. Therefore, the settings for each are covered separately.

You do most Enforcer configuration and administration from the console. Most Enforcer configuration settings can only be changed on the console. However, some Enforcer settings require you to edit an Enforcer file on the Enforcer computer rather than on the console. Almost all settings for Enforcers are set from the Servers page on the console. The LAN Enforcer has a few additional required settings on the Policies page.

See "Configuring an Enforcer appliance" on page 805.

If you administer multiple Enforcers and are responsible for other tasks, it is generally more convenient to administer them all in one centralized location. The console provides this capability. You can log on to a console to display information about all Enforcers.

You must perform a few tasks on the computer on which the Enforcer is installed. The tasks include using the Enforcer local console rather than the management console and hardware maintenance tasks. For example, you troubleshoot an Enforcer and a console connection on the Enforcer itself. To define the problem, you may need to physically check the status of the Enforcer computer hardware or change its network connection.

This chapter does not include information on how to configure the Symantec Enforcement client, which is a separate component from the Enforcer.

About managing Enforcers from the Servers page

The **Servers** page on the management console lists installed Enforcers, along with connected servers and consoles, in the **View Servers** pane. Each Enforcer is listed under a group name. You edit Enforcer properties at the group level.

See "Changing an Enforcer's name and description" on page 972.

You need full system administrator privileges to view the **Servers** page.

About Enforcer groups

Enforcer configuration on the console is done at the Enforcer group level rather than at the individual Enforcer level. Enforcers are listed under a group name on the console Servers page.

Enforcer groups are a way to synchronize Enforcer settings. All Enforcers in a group share the same settings (properties). To update the Enforcer properties, you must select the group name in the **Servers** pane and edit the group properties.

See "Setting up an Enforcer group name on the Symantec Integrated Enforcer for Microsoft Network Access Protection console" on page 1038.

How the console determines the Enforcer group name

When you set up the console connection on the Enforcer local console, you can specify a group name. The Enforcer registers itself with the console after establishing the connection. The console automatically assigns the Enforcer to the specified group and lists the Enforcer under the group name in the console **Servers** pane. If you do not specify a name during setup, the console assigns the Enforcer to a default Enforcer group. The console uses the name of the Enforcer computer as the group name.

See "Setting up an Enforcer group name on the Symantec Integrated Enforcer for Microsoft Network Access Protection console" on page 1038.

About failover Enforcer groups

A new Enforcer identifies itself to the console as a standby failover Enforcer. This identification happens if you add a failover Gateway Enforcer that connects by a hub or switch to the same subnet. The console then assigns the new standby failover Enforcer to the same group as the active Enforcer. The assignment occurs whether or not you specified a group name during setup on the local console. This action ensures that the failover Gateway Enforcer has exactly the same settings as the primary Enforcer.

See "Failover planning for Gateway Enforcer appliances" on page 866.

For LAN Enforcers, failover is handled through the switch rather than through the Enforcer so the automatic assignment to the same group does not occur. You can ensure that multiple LAN Enforcers share settings. Specify the same group name in the Enforcer local console on the console **Settings** dialog box.

See "Planning for the installation of a LAN Enforcer appliance" on page 909.

About changing a group name

You cannot change an Enforcer group name from the console. However, you can specify a new group name from the Enforcer local console. The Enforcer then moves into the new group. You may need to refresh the console screen to see the change.

See "How the console determines the Enforcer group name" on page 969.

About creating a new Enforcer group

Usually, you only need to create a new Enforcer group if you add an Enforcer that required different settings from the existing Enforcers.

You can create a new Enforcer group on the Enforcer local console by specifying the new name on the console **Settings** dialog box. The new group has the Enforcer default settings.

You can leave the group name field blank when you connect the new Enforcer from the local console. In that case, the console assigns the Enforcer to a new group. This group takes the name of the Enforcer computer and its default settings.

You can use the same method to move an Enforcer to another group. Specify the desired group name from the Enforcer local console. The Enforcer takes on the settings of the group to which it is moved.

See "Adding or editing the name of a LAN Enforcer appliance group with a LAN Enforcer" on page 923.

See "Adding or editing the name of an Enforcer group for Symantec Network Access Control Integrated Enforcer" on page 1011.

About the Enforcer information that appears on the Enforcer console

You can display information about the Enforcer on the Enforcer console.

You can only change the settings for network interface cards on the Enforcer appliance but not on the management console. If you change the NIC configuration on the Enforcer appliance, the new settings are uploaded to the management console during the next heartbeat.

See "Displaying information about the Enforcer on the management console" on page 971.

Table 50-1 describes the type of information that you can view.

Table 50-1   Information about the Enforcer appliance on the management
console

Field	Description
Name	Same as Hostname field.
Description	Brief description of the Enforcer. The description is the only information that you can be edit on the management console.
Version	Version of the Enforcer software that runs on the selected Enforcer computer.
Hostname	Name of the computer on which the Enforcer is installed.
Operating System	Operating system that is running on the computer on which the selected Enforcer is installed.
Online Status	Online: The service is running and is the primary active Enforcer. Offline: The service is stopped.
Failover Status	(Gateway Enforcer only) Whether the Enforcer is active or on standby.
Internal IP	IP address of the internal network interface card.
External IP	(Gateway Enforcer only) IP address of the external network interface card.
Internal MAC	The MAC address of the internal network interface card.
External MAC	(Gateway Enforcer only) The MAC address of the external network interface card.
Internal NIC	Manufacturer and model of the internal network interface card.
External NIC	(Gateway Enforcer only) Manufacturer and model of the external network interface card.

Displaying information about the Enforcer on the management console

You can display information about the Enforcer from a management console.

See "About the Enforcer information that appears on the Enforcer console"
on page 970.

To display information about the Enforcer on the management console

1   In the Symantec Endpoint Protection Manager Console, on the **Admin** page, click **Servers**.

2   Under **Servers**, click the name of the Enforcer about which you want to view information.

    Information about the LAN Enforcer appliance does not appear in the fields that refer to the external NIC because the LAN Enforcer appliance only requires an internal NIC. No failover status is shown because a switch manages LAN Enforcer failover.

Changing an Enforcer's name and description

The Enforcer name is always the host name of the appliance or computer on which it is installed. You can only change the Enforcer name by changing the host name of the computer.

You can change the Enforcer description from the console. For example, you may want to enter a description to identify the Enforcer location.

To change an Enforcer's description

1   In the Symantec Endpoint Protection Manager Console, on the **Admin** page, click **Servers**.

2   Under **Servers**, click the Enforcer name and then under **Tasks**, click **Edit Enforcer Properties**. The **Properties** dialog box appears. The name field is not editable.

3   Enter the desired text in the **Description** text box.

4   Click **OK**.

    You can also edit the Enforcer description by right-clicking the name of the Enforcer and selecting **Properties**.

Deleting an Enforcer or an Enforcer group

You can delete an Enforcer on the management console. When you delete an Enforcer, it frees up a license because the computer being used is no longer running an Enforcer. You cannot delete an Enforcer from the console while the Enforcer is online. You can turn off the Enforcer and then delete it. When you restart the Enforcer computer, the Enforcer reconnects to the console. The Enforcer registers itself again and reappears on the **Servers** page. To delete an Enforcer permanently from the console, first uninstall the Enforcer from the Enforcer computer.

To delete an Enforcer group after you uninstalled the Enforcer from the Enforcer computer

1   Turn off or uninstall the Enforcer on the Enforcer computer.

2   In the Symantec Endpoint Protection Manager Console, on the **Admin** page, click **Servers**.

3   Under **Servers**, click the Enforcer name, and then under **Tasks**, click **Delete Enforcer**. A message box asks you to confirm the deletion.

4   To confirm the deletion, click **Yes**.

    If there are no Enforcers listed in an Enforcer group and you no longer want to use that group, you can delete the Enforcer group. The group must no longer include any names of Enforcers before you can delete it. When you delete an Enforcer group, you delete any customized settings for the group.

To delete an Enforcer group

1   In the Symantec Endpoint Protection Console, click **Admin**.

    In the **Admin** page, click **Servers**.

2   Under **Servers**, click the Enforcer group name.

3   Click **Delete Group**.

    A message box asks you to confirm the deletion.

4   To confirm the deletion, click **Yes**.

Exporting and importing Enforcer group settings

You may want to export or import settings for an Enforcer group. Settings are exported to a file in .xml format. When you import settings, you must import them into an existing Enforcer group, which overwrites the selected group settings.

To export Enforcer group settings

1   In the Symantec Endpoint Protection Manager Console, on the **Admin** page, click **Servers**.

2   Under **Servers**, click the Enforcer group name and then click **Export Group Properties**.

3   Select a location in which to save the file and specify a file name.

4   Click **Save**.

To import Enforcer group settings

1   In the Symantec Endpoint Protection Manager Console, on the **Admin** page, click **Servers**.

2   Under **Servers**, click the Enforcer group name whose settings you want to overwrite and then click **Import Group Properties**.

3   Select the file that you want to import and then click **Open**.

You are prompted to confirm overwriting the current Enforcer group properties.

4   Click **Yes**.

Pop-up messages for blocked clients

When an Enforcer blocks a client that tries to connect to the network, the following two types of pop-up messages can be configured:

■   Message for the computers that are running a client

■   Message for Windows computers that are not running a client (Gateway Enforcer only)

Messages for the computers that are running the client

If the Enforcer blocks computers even though they are running a client, there can be several causes. A blockage can occur because a Host Integrity check failed or because the client policy is not up-to-date. When these events occur, you can specify that a pop-up message displays on the client. That message notifies the user that the Enforcer has blocked all traffic from the client and why it was blocked. For example, the following message is displayed if the client has failed the Host Integrity check:

```
Symantec Enforcer has blocked all traffic from the client because
the client failed Host Integrity.
```

You can add text to the default message. For example, you may want to tell the computer user what to do to remedy the situation. You configure this message as part of the client group policy settings rather than the Enforcer settings.

Messages for Windows computers that are not running the client (Gateway Enforcer only)

In some cases, clients try to connect to the enterprise network without running the client. The Gateway Enforcer provides a pop-up message to inform users on

Windows computers of the need to install the client software. The message tells the clients that they are blocked from accessing the network because the Symantec client is not running. You can configure the contents of the message on the **Authentication** tab of the Enforcer **Settings** dialog box. Use the Enable pop-up message option on the client if client is not running.

Note: An alternative to the pop-up message is the HTTP Redirect option. The HTTP Redirect option connects the client to a Web site with remediation instructions or capabilities.

For the Enforcer to cause the client to display a message, UDP ports 137 and 138 must be open to transmit the message.

Windows Messaging, also called Messenger, must be running on Windows NT-based systems (Windows NT 4.0, 2000, XP, and Windows Server 2003) for the computer to display pop-up messages. If the client is running, Windows Messaging is not required for displaying a pop-up message from the client.

Setting up the Enforcer messages

You can configure the Enforcer messages that appear on the clients when an Enforcer blocks the clients.

Note: You can modify the settings only for the groups that do not inherit settings from a parent group.

To set up the Enforcer messages

1   In the Symantec Endpoint Protection Manager Console, on the **Clients** page, select the **Policies** tab.

2   Under **View Policies**, select the group for which you want to specify a pop-up message.

3   Under **Settings**, select **General Settings**. The **Group Settings** dialog box appears with the **General Settings** tab selected.

4   On the **Security Settings** tab, select **Display a message when a client is blocked by a Symantec Enforcer**.

5   If you want to add text to the default message, click **Set Additional Text**, then type the text, and click **OK**.

6   Click **OK**.

About client settings and the Enforcer

Symantec clients work with the Enforcer without special configuration. The exception is some 802.1x authentication settings required for the LAN Enforcer.

Configuring clients to use a password to stop the client service

The client can pass Enforcer authentication initially, while the client is running, and receive a normal network configuration and IP address. If the client later fails authentication, the Enforcer sends a message to the client. This failure causes the client to release and renew the IP address. However, if the end user stops the client on the client computer, the Enforcer is unable to enforce the release and renew. To ensure that the Enforcer can continue to quarantine or block clients, you may want to restrict which users are allowed to stop a client. You can restrict users by requiring a password for the end user to stop the client.

To configure clients to use a password to stop the client service

1   In the Symantec Endpoint Protection Manager Console, on the **Client** page, select the client group.

2   On the **Policies** tab, under Settings, click **General Settings**.

3   On the **Security Settings** tab, under **Client Password Protection**, select **Require a password to stop the client service** and specify the password.

4   Click **OK**.

About Enforcer reports and logs

Enforcer reports and logs let you view Enforcer client activities and how the Enforcers flow through your system. For detailed information about the types reports and logs and how to view them, see Symantec Endpoint Protection Manager Help.

The **Reports** page on the Symantec Endpoint Protection Manager console provides both predefined reports and custom reports. You can view the predefined Quick Reports that contain information about Enforcers on the **Reports** page.

The following Enforcer reports are available:

■   The System report that is called Top Enforcers That Generate Errors contains information about Enforcers that generated errors and warnings.

- The System report that is called Site Status contains information about Enforcer system, traffic, and packet log throughput.

- The Compliance reports contain information about the compliance status of clients.

Enforcer logs include the data that you can use to monitor and troubleshoot system activity:

The following types of Enforcer logs are available:

- Enforcer Server log. This log contains the information that is related to the functioning of an Enforcer.

- Enforcer Client log. This log contains information about interactions between an Enforcer and clients trying to connect to the network.

- Enforcer Traffic log (Gateway Enforcer only). This log records all traffic that enters through a Gateway Enforcer appliance's external adapter and leaves through the internal adapter.

- Enforcer Activity log. This log contains information about events such as when Enforcers start and when they connect to the Symantec Endpoint Protection Manager.

By default, Enforcer logs are stored on the same computer on which the Enforcer software is installed or on the Enforcer appliance itself. You can have the logs automatically sent from the Enforcer appliance or the computer on which you installed an Integrated Enforcer to the Symantec Endpoint Protection Manager Console. However, you must enable the sending of the logs on the Symantec Endpoint Protection Manager Console.

The log data is sent from the Enforcer to the Symantec Endpoint Protection Manager and stored in the database. You can modify the Enforcer log settings, view Enforcer logs, and generate reports about the Enforcers on the Symantec Endpoint Protection Manager Console. Activities are recorded in the same Enforcer Server log for all Enforcers on a site.

For detailed information about the types of reports and logs and how to view them, see Symantec Endpoint Protection Manager Help.

Configuring Enforcer log settings

You can configure settings for Enforcer logs on the *Enforcer name* **Settings** dialog box on the **Logging** tab. The changes are sent to the selected Enforcer during the next heartbeat.

To configure Enforcer logs

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

3 Under **Servers**, select the Enforcer group for which you want to change log settings.

4 Under **Tasks**, click **Edit Group Properties**.

5 In the *Enforcer name* **Settings** dialog box, on the **Logging** tab, change any of the following:

Disable logging on the Symantec Endpoint Protection Manager Console	Uncheck **Enable logging** for each log that you want to disable.
Enable the sending of Enforcer logs from an Enforcer to the Symantec Endpoint Protection Manager	Check **Send the log to the management server**.
Set up the size and age of logs	In each of the **Maximum log file size** fields, specify that number of kilobytes of data to maintain in each log.
	In the **Log entry will expire after** field, specify the number of days that the entry remains in the database before it is removed. The range is 1 to 365 days.
Filter the Enforcer traffic log	Select one of the following filter options: ■ **All traffic** to log all traffic including that which is allowed and that which is dropped. ■ **Only blocked traffic** to log only the clients that the Enforcer blocks. ■ **Only allowed traffic** to log only the traffic that the Enforcer allows.

6 Click **OK**.

See "About Enforcer reports and logs" on page 976.

Disabling Enforcer logging on the Symantec Endpoint Protection Manager Console

By default, Enforcer logging is enabled. You can disable it on the Symantec Endpoint Protection Manager Console. If you disable logging, you can enable it from this same location.

To disable Enforcer logging on the Symantec Endpoint Protection Manager Console

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **Servers**, select the Enforcer group for which you want to disable Enforcer logging.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the *Enforcer name* **Settings** dialog box, on the **Logging** tab, uncheck **Enable logging** for each log that you want to disable.

6   Click **OK**.

See "About Enforcer reports and logs" on page 976.

Enabling the sending of Enforcer logs from an Enforcer to the Symantec Endpoint Protection Manager

All logs are automatically sent by default from the Enforcer appliance or the computer on which you installed any of the software-based Integrated Enforcer to the Symantec Endpoint Protection Manager. As soon as you enable the sending of logs, you can view all Symantec logs in a central location on the Symantec Endpoint Protection Manager Console.

To enable the sending of Enforcer logs from an Enforcer to the Symantec Endpoint Protection Manager

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **Servers**, select the Enforcer group for which you want to enable the sending of Enforcer logs from an Enforcer to a Symantec Endpoint Protection Manager.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the *Enforcer name* **Settings** dialog box, on the **Logging** tab, check **Send the log to the management server**.

You can enable the sending of each type of log from an Enforcer appliance or a computer on which you installed any of the software-based Integrated Enforcers to the Symantec Endpoint Protection Manager.

6   Click **OK**.

See "About Enforcer reports and logs" on page 976.

Setting up the size and age of Enforcer logs

You can specify the maximum size of Enforcer log files and how many days log entries are stored.

To set up the size and age of Enforcer logs

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **Servers**, select the Enforcer group for which you want to set the size and age of Enforcer logs.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the *Enforcer name* **Settings** dialog box, on the **Logging** tab, in each of the Maximum log file size fields, specify the number of KB of data to maintain in each log.

You can enter a size between 64 KB and 2 GB. The default setting is 512 KB.

6   In the **Log entry will expire after** field, specify the number of days that the entry remains in the database before it is removed.

The range is 1 day to 365 days, with a default range of 30 days.

7   Click **OK**.

See "About Enforcer reports and logs" on page 976.

Filtering the Traffic logs for an Enforcer

If you have many clients that connect through an Enforcer, it may generate a large Traffic log. You can filter the type of data that an Enforcer logs in a Traffic log and thus reduce the average log size. The filter list enables you to filter the traffic that an Enforcer logs before the data is retained.

To filter the Traffic logs for an Enforcer

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **Servers**, select the Enforcer group for which you want to filter Traffic logs.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the *Enforcer name* **Settings** dialog box, on the **Logging** tab, in the Traffic log filter list, select one of the following filter options:

All traffic	Logs all traffic, including that which is allowed and dropped
Only blocked traffic	Logs only the clients that the Enforcer blocks
Only allowed traffic	Logs only the traffic that the Enforcer allows

6   Click **OK**.

See "About Enforcer reports and logs" on page 976.

Using the syslog server to monitor an Enforcer

You can use the syslog facility to log Enforcer messages. You can specify the following aspects:

- IP address of the syslog server

- Level of syslog entry

- Authentication failure threshold

- Alive message interval

To enable logging messages to the syslog for an Enforcer

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **Servers**, select the Enforcer group for which you want to enable logging to the syslog.

4   Under **Tasks**, click **Edit Group Properties.**

5 On the **Logging** tab, in the **Syslog** section, select among the following options:

Syslog server	Specify the IP address of the syslog server.
Level	The default level of syslog entry is Information. The levels include: Notice and Information. All logs more serious than the level specified are uploaded to the log server.
Authentication failure threshold	This parameter is defined in terms of the number of times multiples by the number of seconds. When authentication fails more frequently than specified, the following messages are logged.
Alive message interval	The Enforcer sends an "alive" message to the syslog server at a specified interval, in seconds. The default value is 1800 seconds.

6 Click **OK**.

Introducing the Symantec Integrated Enforcers

This chapter includes the following topics:

- About the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers

- About the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection

About the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers

The Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers works in concert with the Microsoft Dynamic Host Configuration Protocol (DHCP) server. It ensures that the clients that try to connect to the network comply with configured security policies.

The Integrated Enforcer for Microsoft DHCP Servers achieves security by intercepting and checking DHCP messages from each client that receives a dynamic IP address through the DHCP server. It then groups non-secure computers into a quarantine class and provides non-secure computers with available, limited resources for each established policy configuration.

About the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection

The Integrated Enforcer for Microsoft Network Access Protection (NAP) works in concert with the Microsoft Windows Network Policy Server (NPS) on a Microsoft Windows Server 2008 and Windows Server 2008 R2. The Symantec Integrated NAP Enforcer ensures that the clients that try to connect to the network comply with configured security policies.

NAP restricts access to networks by creating a controlled environment. It checks the security posture of a client before the client can connect to the enterprise network. If a client is noncompliant, NAP either corrects the security posture or limits access to endpoints that do not meet a company's security policy.

Network Access Protection is a client "security health policy" creation, enforcement, and remediation technology that is included in the Windows Server 2008 operating system. System administrators can create and automatically enforce security policies. These security health policies may include software requirements, security update requirements, required computer configurations, and other settings. Client computers that are not in compliance with a security health policy can be provided with restricted network access. When their configuration is updated and brought into compliance with a policy, clients have full network access. Depending on how you deploy NAP, noncompliant clients can be automatically updated so that users regain full network access without manually updating or reconfiguring their computers.

Note: Microsoft uses "security health policy" in its documentation for Network Access Protection. Symantec uses "security policy" and "host integrity policy" to mean the same thing.

See "How an Integrated Enforcer for Microsoft Network Access Protection works with a Microsoft Network Policy Server (NPS)" on page 792.

Installing the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers

This chapter includes the following topics:

- Process for installing the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers

- System requirements for an Integrated Enforcer for Microsoft DHCP Servers

- Components for an Integrated Enforcer for Microsoft DHCP servers

- Placement requirements for an Integrated Enforcer for Microsoft DHCP Servers

- How to get started with the installation of an Integrated Enforcer for Microsoft DHCP servers

- Installing an Integrated Enforcer for Microsoft DHCP Servers

Process for installing the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers

Table 52-1 lists the steps to install the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers.

Table 52-1   Installation summary for the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers

Step	Action	Description
Step 1	Read the system requirements and the installation requirements.	Identifies the hardware, software, and Symantec Network Access Control components you need to obtain to run the Enforcer and helps you plan for its placement on your network. See "System requirements for an Integrated Enforcer for Microsoft DHCP Servers" on page 986. See "Components for an Integrated Enforcer for Microsoft DHCP servers" on page 987.
Step 2	Install the Symantec Endpoint Protection Manager.	Installs the application that you use to support the Enforcer on your network.
Step 3	Install the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers.	Installs the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers components. See "Installing an Integrated Enforcer for Microsoft DHCP Servers" on page 991.

System requirements for an Integrated Enforcer for Microsoft DHCP Servers

Table 52-2 summarizes the minimum requirements for the computers on which you install the Integrated Enforcer for Microsoft DHCP Servers.

Table 52-2   Integrated Enforcer for Microsoft DHCP Servers system requirements

Component	Requirement
Hardware	For installations of up to 10,000 users, use the following recommended requirements: ■ Pentium III 750 MHz ■ 256 MB of memory ■ 120 MB of disk space ■ Fast Ethernet network adapters ■ One network interface card (NIC) with TCP/IP installed For installations of 10,000 users or greater, use the following recommended requirements: ■ Pentium 4 2.4 GHz ■ 512 MB of memory ■ 512 MB of disk space ■ 1-GB network adapters ■ 800 x 600 resolution monitor with 256 colors (minimum) ■ One network interface card (NIC) with TCP/IP installed
Operating system	The Integrated Enforcer requires that the Microsoft DHCP server and the following 32-bit and 64-bit operating systems are installed: ■ Windows Server 2003 Service Pack ■ Windows Server 2003 Service Pack 1 ■ Windows Server 2003 x64 ■ Windows Server 2008 ■ Windows Server 2008 x64 ■ Windows Server 2008 R2

Components for an Integrated Enforcer for Microsoft DHCP servers

The Integrated Enforcer for Microsoft DHCP servers works with the Microsoft DHCP server, the Symantec Endpoint Protection Manager, and the Symantec Network Access Control client. It verifies that the clients that try to connect to the network comply with configured security policies.

Table 52-3 shows the components that are required for using the Integrated Enforcer for Microsoft DHCP servers:

Table 52-3 Components for Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers

Component	Description
Symantec Endpoint Protection Manager	Creates the security policies in a centralized location and assigns them to clients.
Symantec Network Access Control client	Protects end users by enforcing the security policies that the Integrated Enforcer for Microsoft DHCP servers provides.
Microsoft DHCP server	Provides DHCP addresses to clients.
Integrated Enforcer for Microsoft DHCP servers (installed on the same computer as the DHCP service)	Authenticates clients and enforces security policies.

Placement requirements for an Integrated Enforcer for Microsoft DHCP Servers

Figure 52-1 illustrates how to place the Integrated Enforcer for Microsoft DHCP Servers, the Microsoft DHCP Server, and the Symantec Endpoint Protection Manager, as well as internal or remote clients in a network.

Figure 52-1   Placement of Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers
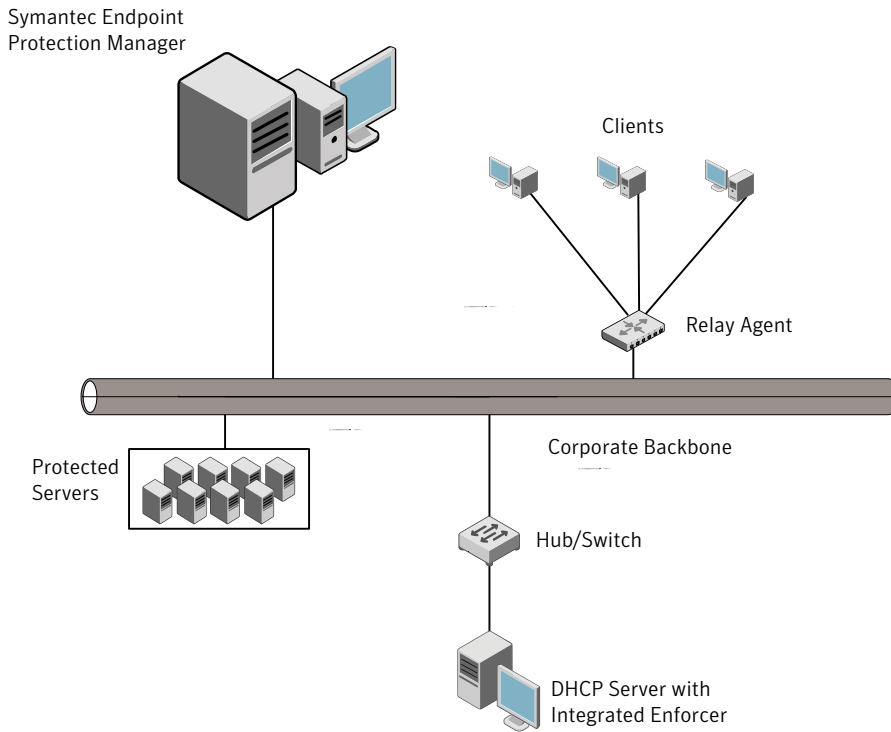
How to get started with the installation of an Integrated Enforcer for Microsoft DHCP servers

The documentation describes how to install, configure, and use the Integrated Enforcer for Microsoft DHCP Servers. Perform the following tasks to get started:

Table 52-4   Process for installing an Integrated Enforcer for Microsoft DHCP servers

Step	Action	Description
Step 1	Locate the Symantec Network Access Control installation components.	Describes the components that are needed for the installation of an Integrated Enforcer for Microsoft DHCP servers. See "Components for an Integrated Enforcer for Microsoft DHCP servers" on page 987.
Step 2	Obtain the required hardware.	Lists the hardware requirements for an Integrated Enforcer for Microsoft DHCP servers. See "System requirements for an Integrated Enforcer for Microsoft DHCP Servers" on page 986.
Step 3	Obtain the required operating system.	Lists the operating system requirements that for an Integrated Enforcer for Microsoft DHCP servers.
Step 4	Place the Integrated Enforcer for Microsoft DHCP servers on your network.	Explains where to place an Integrated Enforcer for Microsoft DHCP servers in a network. See "Placement requirements for an Integrated Enforcer for Microsoft DHCP Servers" on page 988.
Step 5	Install an Integrated Enforcer for Microsoft DHCP server	Explains how to install an Integrated Enforcer for Microsoft DHCP servers. See "Installing an Integrated Enforcer for Microsoft DHCP Servers" on page 991.

Table 52-4		Process for installing an Integrated Enforcer for Microsoft DHCP servers *(continued)*
Step	**Action**	**Description**
Step 6	Configure the Integrated Enforcer for Microsoft DHCP servers	Explains how to configure the connections and settings of an Integrated Enforcer for Microsoft DHCP servers on an Enforcer console. See "About configuring Integrated Enforcers on an Enforcer console" on page 996.

Installing an Integrated Enforcer for Microsoft DHCP Servers

You must install an Integrated Enforcer for Microsoft DHCP servers on the same computer on which you have already installed the Microsoft Windows server operating system along with the DHCP service. You must log in as an administrator or as a user in the administrators group.

Note: After installing the Microsoft DHCP server, you must configure the Integrated Enforcer for Microsoft DHCP servers. The Integrated Enforcer for Microsoft DHCP servers can then connect to the Symantec Endpoint Protection Manager.

To install the Integrated Enforcer for Microsoft DHCP Servers with a Wizard

1   Insert the product disc.

    If the installation does not start automatically, double-click one of::

    ■ **IntegratedEnforcerInstaller86.exe** (for x86 OSes).

    ■ **IntegratedEnforcerInstaller64.exe** (for x64 OSes).

    You must exit the installation and install the DHCP server if you see the following message:

    ```
    You must have the DHCP server on this machine
    to install this product. To install the DHCP server,
    in the Control Panel, use the Add/Remove Windows
    Components Wizard.
    ```

If the DHCP server is already installed, the Welcome to Symantec Integrated Enforcer Installation Wizard appears.

2   In the **Welcome** panel, click **Next**.

3   In the **License Agreement** panel, click **I accept the license agreement**.

4   Click **Next**.

5   In the **Destination Folder** panel, perform one of the following tasks:

   ■   If you want to accept the default destination folder, click **Next**.

   ■   Click **Browse**, locate and select a destination folder, click **OK**, and click **Next**.

6   If the **Role Selection** panel appears, select **DHCP Enforcement for Microsoft DHCP Server** and click **Next**.

   The **Role Selection** panel only appears if more than one type of Symantec Network Access Control Integrated Enforcer can be installed based on the services running on the server.

7   In the **Ready to Install the Application** panel, click **Next**.

8   When asked whether you want to restart the DHCP server, perform one of the following tasks:

   ■   To restart the DHCP server immediately, click **Yes**.

   ■   To restart the DHCP server manually later, click **No**.
       If you restart the DHCP server later, you must stop and then start it.

   You must restart the DHCP server or the Symantec Integrated Enforcer does not function.

   See "Stopping and starting the Microsoft DHCP Server manually" on page 994.

9   Click **Finish**.

   If you need to reinstall the Integrated Enforcer, you must first uninstall it.

   See "Uninstalling the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers" on page 993.

To install the Integrated Enforcer for Microsoft DHCP Servers from the command line

1   To begin the command-line installation, open a DOS command prompt.

   The command-line installation process uses only default settings.

2   At the command line, specify the directory in which the Integrated Enforcer Installer is located.

   The install location defaults to one of:

■ `C:\Program Files\Symantec\Symantec Endpoint Protection\Integrated Enforcer` for x86 OSes.

■ `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Integrated Enforcer` for x64 OSes.

3 Type `IntegratedEnforcerInstaller86.exe /qr` (for x86 OSes) or `IntegratedEnforcerInstaller64.exe /qr` (for x64 OSes) at the command line and type: `Enter`.

Uninstalling the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers

You can uninstall the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers from the Windows taskbar or the command line.

To uninstall the Integrated Enforcer for Microsoft DHCP Servers

1 On the Windows taskbar, click **Start > Control Panel > Add or Remove Programs**.

2 Click **Symantec NAC Integrated Enforcer**, and then click **Remove**.

3 When asked whether you want to remove the software, click **Yes**.

4 When asked whether you want to restart the DHCP server, do one of the following tasks:

■ To restart the DHCP server immediately, click **Yes**.

■ To restart the DHCP server manually later (the default), click **No**.
If you restart the DH
CP server later, you must stop and then start it.
You must restart the DHCP server to completely uninstall the Symantec Integrated Enforcer.

To uninstall the Integrated Enforcer for Microsoft DHCP Servers from the command line

1 Open a DOS command prompt.

2 At the command prompt, type:

`misexec.exe /qn /X <filename >` The filename should be under Program Files\Common Files\Wise Installation Wizard.

Upgrading the Integrated Enforcer for Microsoft DHCP Servers

The following steps detail how to upgrade to a Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Servers:

Table 52-5   Upgrade steps for the Integrated Enforcer for Microsoft DHCP Servers

Step	Action	Description
Step 1	Uninstall the old version.	Uninstall the existing version of the Integrated Enforcer. See "Uninstalling the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers" on page 993.
Step 2	Install the new version.	Install the new version of the Integrated Enforcer. See "Installing an Integrated Enforcer for Microsoft DHCP Servers" on page 991.

Note: Migration is not supported. You must uninstall the old version and install the new one.

Stopping and starting the Microsoft DHCP Server manually

Stop the Microsoft DHCP Server manually before upgrading to a new version of the Integrated Enforcer for Microsoft DHCP Servers. You then restart it after you complete the upgrade.

To stop and start the Microsoft DHCP Server manually

1   On the Windows taskbar, click **Start** > **Control Panel** > **Administrative Tools** > **Services**.

2   Right-click **DHCP Server** and click **Stop**.

3   Click **Start**.

Configuring the Symantec Integrated Enforcers on the Enforcer console

This chapter includes the following topics:

■ About configuring Integrated Enforcers on an Enforcer console

■ Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec Endpoint Protection Manager

■ Configuring automatic quarantine

■ Editing a Symantec Endpoint Protection Manager connection

■ Configuring Integrated Enforcer communication settings in Symantec Endpoint Protection Manager

■ Configuring a trusted vendor list

■ Viewing Enforcer logs on an Enforcer console

■ Stopping and starting communication services between an Integrated Enforcer and a management server

■ Configuring a secure subnet mask

■ Creating DHCP scope exceptions

About configuring Integrated Enforcers on an Enforcer console

After you complete the installation of a Symantec Network Access Control Integrated Enforcer, there are two stages of configuration. First, configure the settings on the Integrated Enforcer console. Second, move to the Symantec Endpoint Protection Manager to make any desired changes to the configuration settings for the group that the Integrated Enforcer is part of.

Table 53-1 outlines these tasks.

Table 53-1   Enforcer console configuration summary

Step	Action	Description
Step 1	Establish a connection between the Integrated Enforcer for Microsoft DHCP Servers and a management server.	Use the Integrated Enforcer console to configure the connection between the Integrated Enforcer for Microsoft DHCP Servers and Symantec Endpoint Protection Manager See "Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec Endpoint Protection Manager" on page 998.
Step 2	Set up the DHCP server with a quarantine configuration.	Use one of two methods to configure a quarantine user class for remediation. See "Configuring automatic quarantine" on page 1000.
Step 3	Restart the DHCP service.	Manually stop and start the DHCP service on the DHCP server. See "Stopping and starting the Microsoft DHCP Server manually" on page 994.
Step 4	Optionally, change Integrated Enforcer basic settings.	Add or edit descriptions for an Integrated Enforcer or group of Integrated Enforcers, or for the Integrated Enforcer IP address or host names. See "Configuring Symantec Network Access Control Integrated Enforcer basic settings" on page 1010.

Table 53-1   Enforcer console configuration summary *(continued)*

Step	Action	Description
Step 5	Connect the Integrated Enforcer to a Symantec Endpoint Protection Manager.	Connect the Integrated Enforcer to a server on which the Symantec Endpoint Protection Manager is installed. See "Connecting the Symantec Network Access Control Integrated Enforcer to a Symantec Endpoint Protection Manager" on page 1012.
Step 6	As needed, update the connection to the Symantec Endpoint Protection Manager.	Update the connection to the Symantec Endpoint Protection server address and port information as required. See "Editing a Symantec Endpoint Protection Manager connection" on page 1002.
Step 7	As needed, configure a trusted vendor list.	Configure a trusted vendor list for devices on your network such as printers or IP telephones. These are the devices that the Integrated Enforcer does not need to authenticate. See "Configuring a trusted vendor list" on page 1004.
Step 8	Optionally, set where you want to view logs.	Set up logs for viewing on the Enforcer console or the Symantec Endpoint Protection Manager. See "Viewing Enforcer logs on an Enforcer console" on page 1005. See "Configuring logs for the Symantec Network Access Control Integrated Enforcer" on page 1023.

Table 53-1   Enforcer console configuration summary *(continued)*

Step	Action	Description
Step 9	Optionally, set authentication settings for your network.	Set up how you want to authenticate clients, servers, and devices. See "Specifying the maximum number of challenge packets during an authentication session" on page 1019. See "Specifying the frequency of challenge packets to be sent to clients" on page 1019. See "Allowing all clients with continued logging of non-authenticated clients" on page 1020. See "Allowing non-Windows clients to connect to a network without authentication" on page 1021. See "Enabling servers, clients, and devices to connect to the network as trusted hosts without authentication" on page 1014.
Step 10	Optionally, validate that clients are running up-to-date policies.	Validate that clients have the most recent policies by comparing the policy serial number received from the client with the policy serial number in the Symantec Endpoint Protection Manager.

Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec Endpoint Protection Manager

You must specify the Symantec Endpoint Protection Manager to which the Integrated Enforcer can connect. After you set up the management server list, you must configure the connection with the encrypted password, group name, and communication protocol. The encrypted password was previously known as a preshared key.

After the Integrated Enforcer connects to a management server, it registers itself automatically.

Configuring the Symantec Integrated Enforcers on the Enforcer console | 999
Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec
Endpoint Protection Manager

See

To establish communication between the Integrated Enforcer console and Symantec Endpoint Protection Manager

1   On the Windows taskbar of the Integrated Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer**.

The Symantec Network Access Control Integrated Enforcer configuration console appears. This main page shows the connection status between the Integrated Enforcer and the Symantec Endpoint Protection Manager. A green light indicates that Integrated Enforcer is actively connected to the management server. A red light indicates that the connection is disconnected.

2   In the left-hand panel, click **Symantec Integrated Enforcer > Configure > Management Server**.

3   In the **Management Server** dialog box, type the IP address or name of the Symantec Endpoint Protection Manager in the **Server address** text field.

You can type an IP address, host name, or domain name. If you want to use a host name or a domain name, ensure that the name resolves correctly with the Domain Name Server (DNS server).

4   In the **Management Server** dialog box, edit the port number that the Integrated Enforcer uses to communicate with the Symantec Endpoint Protection Manager.

The default port number is 8014 for HTTP protocol and 443 for the HTTPS protocol. The HTTPS protocol must be configured identically on the Symantec Endpoint Protection Manager and Integrated Enforcer.

5   In the **Encryption password** text box, type the password of the Symantec Endpoint Protection Manager for your connection.

The Symantec Endpoint Protection Manager and Integrated Enforcer must use the same encrypted password for communication.

To display the letters and numbers of the preshared key instead of asterisks, check **Use Hash Value**. If **Use Hash Value** is turned on, the encryption password must be 32 characters, and must use hexadecimal numbers only.

6 In the **Preferred** group text box, type a name for the Integrated Enforcer group.

If you do not specify a group name, the Symantec Endpoint Protection Manager assigns the Symantec Network Access Control Integrated Enforcer to a default Enforcer group with default settings. The default group name is I-DHCP. However, a Symantec Network Access Control Integrated Enforcer for Microsoft NAP Servers and appliance-based enforcers must each be in a separate group.

You can view the group settings from the Symantec Endpoint Protection Manager console on the **Servers** page.

7 To specify the protocol that the Symantec Network Access Control Integrated Enforcer uses to communicate with the Symantec Endpoint Protection Manager, select **HTTP** or **HTTPS**.

You can only use the HTTPS protocol if the Symantec Endpoint Protection Manager is running Secure Sockets Layer (SSL).

If you select HTTPS and want to require verification of the management server's certificate with a trusted third-party certificate authority, check **Verify certificate when using HTTPs protocol**.

8 Click **Save**.

After the Integrated Enforcer connects to the Symantec Endpoint Protection Manager, you can change most of the configuration settings on the Symantec Endpoint Protection Manager Console. However, the preshared secret or encrypted password must be the same on the Integrated Enforcer and the Symantec Endpoint Protection Manager in order for them to communicate.

Configuring automatic quarantine

The clients that try to connect to the network send a DHCP request to the DHCP server.

Either the Symantec Network Access Control Integrated Enforcer can perform the quarantine configuration based on allowed IP addresses or you can configure a quarantine user class and add resources to it for each subnet from inside the DHCP server. The Integrated Enforcer appends the quarantine user class to all DHCP messages that come from non-compliant or unknown clients. It also renews the requests from the client to the DHCP server. Clients that are trusted are immediately assigned a normal IP address and are not quarantined. Unknown or untrusted clients are quarantined, authenticated, renewed if authentication succeeds, and then assigned a normal IP address.

Access is based on the Host Integrity policy and group settings that are defined in the Symantec Endpoint Protection Manager.

Enter a list of IP addresses that you want to allow quarantined computers to access, even if authentication fails.

To configure automatic quarantine for a Symantec Network Access Control Integrated Enforcer

1   On the Windows taskbar of the Integrated Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer**.

2   In the left-hand panel, click **Symantec Integrated Enforcer > Configure > Automatic Quarantine Configuration**.

3   In the **Automatic Quarantine Configuration** page of the Integrated Enforcer, click **Add** to begin creating an IP address list.

4   Enter an allowed IP address and click **OK** to add the IP address to the list.

5   Click **Add** again to continue adding IP addresses to the list.

6   Modify the **IP Address** list by clicking **Edit, Remove, Remove all, Move Up**, or **Move down**.

7   When all IP Addresses are listed or modified, click **OK** at the bottom of the page to save your configurations.

To set up a quarantine configuration on a DHCP server (advanced optional task)

1   On the DHCP server, click **Start > Administrative Tools > DHCP**.

    To renew the request with a quarantine configuration, the Integrated Enforcer dynamically appends a quarantine DHCP user class to the DHCP messages that come from the non-compliant clients. You define the quarantine user class by adding an ID called: `SYGATE_ENF`. Then you assign the user class various resources, including a gateway IP address, lease time, a DNS server, and enough static routes for remediation.

2   In the tree of the DHCP dialog box, right-click the DHCP server, and click **Define User Classes**.

3   In the **DHCP User Classes** dialog box, click **Add**.

4   In the **New Class** dialog box, type a display name that identifies this quarantine user class as the quarantine configuration, and an optional description.

    For example, you can identify a quarantine user class, such as QUARANTINE.

5   To define a new user class, click the **ASCII** column and type **SYGATE_ENF** in uppercase letters.

6   Click **OK**.

7   Click **Close**.

To configure scope options on a DHCP server (advanced optional task)

1   In the tree, right-click **Server Options**.

2   Click **Configure Options...**.

3   On the **General** tab, check **003 Router** and configure the IP address of the router that is associated with the DHCP relay client.

4   On the **Advanced** tab, in the **Vendor class** drop-down list, click **DHCP Standard Options**.

5   On the **Advanced** tab, in the **User class** drop-down list, click **SNAC_QUARANTINE**.

6   Check **003 Router**.

7   In the **IP address** field, type **127.0.0.1** (recommended). However, it is up to the administrator to decide which router IP to assign to quarantined clients.

8   Check **051 Lease**.

9   Type the hexadecimal value of the lease time in seconds.

   For example, for 2 minutes, type 0x78.

10 Click **OK**.

11 Click **File > Exit**.

Editing a Symantec Endpoint Protection Manager connection

You can update the Symantec Endpoint Protection Manager IP address and port information as required.

To edit a Symantec Endpoint Protection Manager connection

1   On the Windows taskbar of the Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec Integrated Enforcer**

2   In the left-hand panel, expand Symantec Integrated Enforcer.

3   Expand **Configure**.

4   Click **Management Servers**.

5   In the **Management Servers** panel, click **Edit** from the icon column that is located to the right of the management servers list.

6   In the **Add/Edit Management Server** dialog box, type the IP address or name of the Symantec Endpoint Protection Manager in the Server address text field.

You can type an IP address, host name, or domain name. If you want to use a host name or a domain name, the Symantec Network Access Control Integrated Enforcer must connect to a Domain Name Server (DNS) server.

7   Click **OK**.

Configuring Integrated Enforcer communication settings in Symantec Endpoint Protection Manager

Configuring the Symantec Network Access Control Integrated Enforcer is a two-step process. First, you configure the Integrated Enforcer from the Integrated Enforcer console. Secondly, you complete configuration tasks from the Symantec Endpoint Protection Manager to fully set up communications between the enforcer and the management server. The configuration settings are automatically downloaded from the management server to the Integrated Enforcer during the next heartbeat.

See "About configuring Integrated Enforcers on an Enforcer console" on page 996.

To configure Integrated Enforcer communication settings in Symantec Endpoint Protection Manager

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **Servers**, select the group of Enforcers of which the Integrated Enforcer is a member.

4   Select the Integrated Enforcer whose configuration settings need to be changed.

5 Under **Tasks**, click **Edit Group Properties**.

6 In the **Settings** dialog box, change any of the configuration settings.

The Settings dialog box provides the following tabbed categories of configuration settings:

General	Settings for the Enforcer group name, Enforcer group description, and management server list.
	See "Configuring Symantec Network Access Control Integrated Enforcer basic settings" on page 1010.
Authentication	Settings for a variety of parameters that affect the client authentication process.
	See "Configuring Symantec Network Access Control Integrated Enforcer authentication settings" on page 1016.
Advanced	Settings for authentication timeout parameters and DHCP message timeouts: these options are displayed but currently unavailable for Symantec Network Access Control Integrated Enforcer configuration.
	Settings for MAC addresses for the trusted hosts that the Integrated Enforcer allows to connect without authentication (optional).
	Settings for Local Authentication.
	See "Configuring Symantec Network Access Control Integrated Enforcer advanced settings" on page 1013.
Log Settings	Settings for Server logs, Client Activity logs, and specifying log file parameters.
	See "Configuring logs for the Symantec Network Access Control Integrated Enforcer" on page 1023.

Configuring a trusted vendor list

Clients cannot be installed on some network devices such as printers or IP telephones. To allow for those cases, you can configure a trusted vendor list. If the name of the vendor is considered trusted, then the Symantec Network Access Control Integrated Enforcer will not authenticate the device. The devices will obtain normal IP addresses from the DHCP server.

To configure a trusted vendor list

1   On the Windows taskbar of the Integrated Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer**.

2   In the left-hand panel, click **Symantec Integrated Enforcer > Configure > DHCP Trusted Vendors Configuration**.

3   To enable the trusted vendor list, check **Turn on Trusted Vendors**.

When the **Turn on Trusted Vendors** box is checked, Host Integrity will not be enforced for DHCP traffic from the selected trusted vendors.

4   Select the vendors you want to establish as trusted vendors.

5   Click **Save**.

Viewing Enforcer logs on an Enforcer console

The Symantec Network Access Control Integrated Enforcer automatically logs messages in the Enforcer Client log and the Enforcer System log. These Enforcer logs are uploaded to the Symantec Endpoint Protection Manager. The client log provides information about client connections and communication with the Integrated Enforcer. The system log records information that relates to the Integrated Enforcer itself, such as instances of starting and stopping the Enforcer service.

In the Symantec Endpoint Protection Manager, you can enable and disable logging and set log file parameters for the Integrated Enforcer. All logs are enabled and sent to the Symantec Endpoint Protection Manager by default.

To view Enforcer logs on an Enforcer console

1   In the left pane, expand **Symantec NAC Integrated Enforcer**.

2   Expand **View Logs**, and click **System Log** or click **Client Log**.

3   To view any changes to the log since you last opened the log, click **Refresh**.

4   Click **OK**.

Stopping and starting communication services between an Integrated Enforcer and a management server

For troubleshooting purposes, you can stop and start either the Enforcer service or the service (SNACLink.exe) that communicates with the Symantec Endpoint Protection Manager. If you stop the Enforcer service, the Integrated Enforcer removes the compliance information for existing clients. It also stops collecting information for new clients. However, it continues to communicate with a Symantec Endpoint Protection Manager.

If the Symantec Endpoint Protection Manager is unavailable, the Integrated Enforcer still enforces the policy version and GUID for all authenticated clients. The same process is followed if you stop the connection to the Symantec Endpoint Protection Manager. This information is stored in the local cache (but only if cache is enabled). It automatically authenticates new clients (based on their host integrity status) but it skips the GUID and policy verification.

As soon as the communication to the Symantec Endpoint Protection Manager is reestablished, the Integrated Enforcer updates the policy version. It also authenticates the clients that have been added since the connection was lost.

Note: You can configure the Symantec Network Access Control Integrated Enforcer to quarantine new clients instead of authenticating them while the Symantec Endpoint Protection Manager connection is unavailable. You accomplish this goal by changing the default value of the DetectEnableUidCache key in the Windows registry.

Stopping the Integrated Enforcer does not stop the DHCP server. If the Integrated Enforcer is stopped, the DHCP server functions as if no Enforcer was ever installed. If the DHCP server becomes unavailable, the Integrated Enforcer stops collecting the compliance status about new clients. However, it continues to communicate with existing clients and continues to log status changes. The DHCP server may become unavailable because of maintenance and other problems.

To stop and start the communication services between an Integrated Enforcer and a management server

1   Start the Symantec Network Access Control Integrated Enforcer.

2   Click **Symantec NAC Integrated Enforcer**.

3 You can stop or start either the Enforcer service (`IntegratedEnf.exe`) or the service (`SNACLink.exe`) that communicates with the Symantec Endpoint Protection Manager.

Perform one or both of the following tasks:

■ In the Enforcer service group box, click **Stop**.
This option stops the Enforcer service.

■ In the Management server communication service group box, click **Stop**.
This option stops the Enforcer service that connects to the Symantec Endpoint Protection Manager.

If the status is set to Stopped, the service is not running.

4 To restart either service, click **Start**.

If you turn off or restart the computer to which a Symantec Network Access Control Integrated Enforcer is connected, the Enforcer service restarts automatically when the computer restarts.

If the server communication service is stopped and subsequently restarted, the Symantec Network Access Control Integrated Enforcer tries to connect to a Symantec Endpoint Protection Manager to which it last connected. If that Symantec Endpoint Protection Manager is unavailable, the Integrated Enforcer connects to the first management server that is listed in the management server list.

Configuring a secure subnet mask

The Integrated Enforcer Advanced Settings configuration page allows users to configure a secure subnet mask for quarantined clients.

To configure a secure subnet mask

1 On the **Advanced Settings** configuration page, check the option to **Use secure subnet mask (255.255.255.255) for quarantine IP address**, or click to clear the configuration. If you clear the configuration, you will use the normal DHCP subnet mask.

2 Click **OK** to save your configuration.

Note: The secure subnet mask (`255.255.255.255`) option is only available with the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP servers. If it is turned on, the `255.255.255.255` is used for quarantined clients. If it is turned off, the default subnet mask for the current scope will be used.

Creating DHCP scope exceptions

The Integrated Enforcer Advanced Settings configuration page allows users to manipulate the subnet mask to bypass quarantine. The default configuration at installation is that all DHCP scopes will be enforced for quarantine.

To select subnets for exemption from quarantine

1   On the **Advanced Settings** configuration page, check the option to **Use secure subnet mask (255.255.255.255) for quarantine IP address**

2   Under **Select scopes to be enforced**, click to clear the IP address ranges you want to exempt. IP addresses that belong to the DHCP scopes that are checked will be enforced.

When a DHCP cope is changed to exempt a scope (by clicking to clear the IP address range), IP addresses that have already been assigned to clients will still be enforced. To clear the enforcement, Release and Renew the IP addresses.

Note: If new scope is created or added after the Enforcer is installed, the new scope will not be enforced until it is selected in the user interface on the **Advanced Settings** configuration page.

3   When you are satisfied with your settings, click **OK** to save the configuration.

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint Protection Manager

This chapter includes the following topics:

- About configuring the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint Protection Manager

- Configuring Symantec Network Access Control Integrated Enforcer basic settings

- Configuring Symantec Network Access Control Integrated Enforcer advanced settings

- Configuring Symantec Network Access Control Integrated Enforcer authentication settings

- Configuring logs for the Symantec Network Access Control Integrated Enforcer

About configuring the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint Protection Manager

If you want to support the Symantec Integrated Enforcer for Microsoft DHCP Server in a network environment, you must have a DHCP server set up and running. Most of the configuration takes place on the Enforcer console. Once installed, you can configure the following areas from the Symantec Endpoint Protection Manager

- Configuration, both basic and advanced
  See "Configuring Symantec Network Access Control Integrated Enforcer basic settings" on page 1010.
  See "Configuring Symantec Network Access Control Integrated Enforcer advanced settings" on page 1013.
- Authentication
  See "Configuring Symantec Network Access Control Integrated Enforcer authentication settings" on page 1016.
- Logs
  See "Configuring logs for the Symantec Network Access Control Integrated Enforcer" on page 1023.

Configuring Symantec Network Access Control Integrated Enforcer basic settings

You can add or edit the description of a Symantec Network Access Control Integrated Enforcer or an Integrated Enforcer group in Symantec Endpoint Protection Manager. You can also add or edit them on the Integrated Enforcer console.

See "Adding or editing the description of an Enforcer group with a Symantec Network Access Control Integrated Enforcer" on page 1011.

See "Adding or editing the description of a Symantec Network Access Control Integrated Enforcer" on page 1012.

However, you cannot add or edit the name of an Integrated Enforcer group in the Symantec Endpoint Protection Manager Console. You cannot add or edit the IP address or host name of an Integrated Enforcer in the Symantec Endpoint Protection Manager Console. Instead, you must perform these tasks on the Enforcer console.

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint 1011
Protection Manager
Configuring Symantec Network Access Control Integrated Enforcer basic settings

See "Adding or editing the name of an Enforcer group for Symantec Network Access Control Integrated Enforcer" on page 1011.

You must connect the Integrated Enforcer to a Symantec Endpoint Protection Manager.

See "Connecting the Symantec Network Access Control Integrated Enforcer to a Symantec Endpoint Protection Manager" on page 1012.

Adding or editing the name of an Enforcer group for Symantec Network Access Control Integrated Enforcer

You can add or edit the name of an Enforcer group of which an Integrated Enforcer is a member. You perform these tasks on the Enforcer console during the installation. Later, if you want to change the name of an Enforcer group, you can do so on the Enforcer console.

See "Establishing or changing communication between an Integrated Enforcer for Microsoft DHCP servers and a Symantec Endpoint Protection Manager" on page 998.

All Enforcers in a group share the same configuration settings.

Adding or editing the description of an Enforcer group with a Symantec Network Access Control Integrated Enforcer

You can add or edit the description of an Enforcer group of which a Symantec Network Access Control Integrated Enforcer is a member. You can perform this task on the Symantec Endpoint Protection Manager console instead of the Integrated Enforcer console.

To add or edit the description of an Enforcer group with a Symantec Network Access Control Integrated Enforcer

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **Servers**, select and expand the Enforcer group whose name you want to add or edit.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Settings** dialog box, on the **General** tab, add or edit a description for the Enforcer group in the **Description** field.

6   Click **OK**.

Adding or editing the description of a Symantec Network Access Control Integrated Enforcer

You can add or edit the description of a Symantec Network Access Control Integrated Enforcer. You can perform this task on the Symantec Endpoint Protection Manager console instead of the Integrated Enforcer console. After you complete this task, the description appears in **Description** field of the Management Server pane.

To add or edit the description of a Symantec Network Access Control Integrated Enforcer

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the Enforcer group that includes the Integrated Enforcer whose description you want to add or edit.

4   Select the Integrated Enforcer whose description you want to add or edit.

5   Under **Tasks**, click **Edit Enforcer Properties**.

6   In the **Enforcer Properties** dialog box, add or edit a description for the Integrated Enforcer in the **Description** field.

7   Click **OK**.

Connecting the Symantec Network Access Control Integrated Enforcer to a Symantec Endpoint Protection Manager

Enforcers must be able to connect to servers on which the Symantec Endpoint Protection Manager is installed. The management server includes a file that helps manage the traffic between clients, management servers, and optional Enforcers such as an Integrated Enforcer. This file is called a management server list.

The management server list specifies to which Symantec Endpoint Protection Manager an Integrated Enforcer connects. It also specifies to which Symantec Endpoint Protection an Integrated Enforcer connects in case of a management server's failure.

A default management server list is automatically created for each site during the initial installation. All available management servers at that site are automatically added to the default management server list.

A default management server list includes the management server's IP addresses or host names to which Integrated Enforcers can connect after the initial installation. You may want to create a custom management server list before you deploy any Enforcers. If you create a custom management server list, you can

specify the priority in which an Integrated Enforcer can connect to management servers.

You can select the specific management server list that includes the IP addresses or host names of those management servers to which you want the Integrated Enforcer to connect. If there is only one management server at a site, then you can select the default management server list.

See "Configuring a management server list" on page 740.

To select the management server list for the Symantec Network Access Control Integrated Enforcer

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the group of Enforcers.

    The Enforcer group must include the Integrated Enforcer for which you want to change the IP address or host name in a management server list.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Settings** dialog box, on the **General** tab, under **Communication**, select the management server list that you want this Integrated Enforcer to use.

6   On the **General** tab, under **Communication**, click **Select**.

    You can view the IP addresses and host names of all available management servers, as well as the priorities that have been assigned to them.

7   In the **Management Server List** dialog box, click **Close**.

8   In the **General** dialog box, click **OK**.

Configuring Symantec Network Access Control Integrated Enforcer advanced settings

You can configure the following Integrated Enforcer advanced configuration settings:

■   Timeout parameters, Authentication timeout, and DHCP message timeout
    Although these options are displayed, they are currently unavailable for Symantec Network Access Control Integrated Enforcer configuration.

■   MAC addresses for the trusted hosts that the Integrated Enforcer allows to connect to the normal DHCP server without authentication

■   Enabling local authentication

■ Symantec Endpoint Protection Manager health check

When you apply any of these configuration settings, the changes are sent to the selected Symantec Network Access Control Integrated Enforcer during the next heartbeat.

See "Enabling servers, clients, and devices to connect to the network as trusted hosts without authentication" on page 1014.

See "Enabling local authentication on the Integrated Enforcer" on page 1015.

Enabling servers, clients, and devices to connect to the network as trusted hosts without authentication

A trusted host is typically a server that cannot install the client software such as a non-Windows server, or a device, such as a printer. You may also want to identify non-Windows clients as trusted hosts because the Integrated Enforcer is unable to authenticate any clients that do not run the Symantec Endpoint Protection client or the Symantec Network Access Control client.

You can use MAC addresses to designate certain servers, clients, and devices as trusted hosts.

When you designate servers, clients, and devices as trusted hosts, the Integrated Enforcer passes all DHCP messages from the trusted host without authenticating the trusted host.

To enable servers, clients, and devices to connect to the network as trusted hosts without authentication

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **Servers**, select and expand the group of Enforcers.

4   Select the Integrated Enforcer that permits servers, clients, and the devices that have been designated as trusted hosts to connect to the network without authentication.

5   Under **Tasks**, click **Edit Group Properties**.

6   In the **Settings** dialog box, on the **Advanced** tab, next to **MAC address**, click **Add**.

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint | 1015
Protection Manager
Configuring Symantec Network Access Control Integrated Enforcer advanced settings

7   In the **Add Trusted Host** dialog box, type the MAC address for the client or
the trusted host in the Host MAC address field.

When you specify a MAC address, you can use a wildcard character if you
type it for all three fields on the right.

For example, 11-22-23-*-*-* represents the correct use of the wildcard
character. However, 11-22-33-44-*-66 does not represent the correct use of
the wildcard character.

You can also copy a set of MAC addresses from a text file.

Note: Symantec supports the following format for imports: single MAC
address, and MAC address with mask.

To import MAC addresses, click **Import**. Specify the file in the **Import MAC
Address From File** dialog box.

To export MAC addresses, highlight several MAC addresses, and then click
Export. Specify the file in the **Export MAC Address To File** dialog box.

8   Click **OK**.

Enabling local authentication on the Integrated Enforcer

With local authentication enabled, if the Integrated Enforcer loses its connection
with the client on which the Symantec Endpoint Protection Manager is installed,
the Integrated Enforcer authenticates clients locally. In this case, the Integrated
Enforcer considers the client a valid user and only checks the client's Host Integrity
status.

Note: If the Integrated Enforcer does not lose its connection with the Symantec
Endpoint Protection Manager, it always asks the management server to verify
the client's GUID regardless of whether local authentication is enabled or disabled.

To enable local authentication on the Integrated Enforcer

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **Servers,** select and expand the group of Integrated Enforcers.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Settings** dialog box, on the **Advanced** tab, check **Enable Local Authentication**.

6   Click **OK**.

Configuring Symantec Network Access Control Integrated Enforcer authentication settings

You can specify a number of authentication settings for an Integrated Enforcer authentication session. When you apply these changes, they are automatically sent to the selected Integrated Enforcer during the next heartbeat.

About using authentication settings

You may want to implement a number of authentication settings to further secure the network.

Table 54-1 provides more information about the options on the **Authentication** tab.

Table 54-1   Authentication configuration settings for a Symantec Network Access Control Integrated Enforcer

Option	Description
Maximum number of packets per authentication session	The maximum number of challenge packets that the Integrated Enforcer sends in each authentication session. The default number is 15. See "Specifying the maximum number of challenge packets during an authentication session" on page 1019.
Time between packets in authentication session	The time (in seconds) between each challenge packet that the Enforcer sends. The default value is 4 seconds. See "Specifying the frequency of challenge packets to be sent to clients" on page 1019.

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint | 1017
Protection Manager

Configuring Symantec Network Access Control Integrated Enforcer authentication settings

Table 54-1   Authentication configuration settings for a Symantec Network Access Control Integrated Enforcer *(continued)*

Option	Description
Allow all clients, but continue to log which clients are not authenticated	If this option is enabled, the Enforcer authenticates all users by checking that they are running a client. It then forwards the request to receive a normal rather than a quarantine network configuration, whether the checks pass or fail. The default setting is not enabled. See "Allowing all clients with continued logging of non-authenticated clients" on page 1020.
Allow all clients with non-Windows operating systems	If this option is enabled, the Integrated Enforcer checks for the operating system of the client. The Integrated Enforcer then allows all clients that do not run the Windows operating systems to receive a normal network configuration without being authenticated. If this option is not enabled, the clients receive a quarantine network configuration. The default setting is not enabled. See "Allowing non-Windows clients to connect to a network without authentication" on page 1021.
Check the policy serial number on client before allowing client into network	If this option is enabled, the Integrated Enforcer verifies that the client has received the latest security policies from the management server. If the policy serial number is not the latest, the Integrated Enforcer notifies the client to update its security policy. The client then forwards the request to receive a quarantine network configuration. If this option is not enabled and if the Host Integrity check succeeds, the Integrated Enforcer forwards the Integrated request to receive a normal network configuration. The Integrated Enforcer forwards the Integrated request even if the client does not have the latest security policy. The default setting is not enabled. See "Having the Symantec Network Access Control Integrated Enforcer check the Policy Serial Number on a client" on page 1021.

About authentication sessions

When a client tries to access the internal network, the Symantec Network Access Control Integrated Enforcer first detects whether the client is running a Symantec Endpoint Protection client. If it is, the Enforcer forwards the client DHCP message

to the DHCP server to obtain a quarantine IP address with a short lease time. This process is used internally by the Integrated Enforcer for its authentication process.

The Integrated Enforcer then begins its authentication session with the client. An authentication session is a set of challenge packets that the Integrated Enforcer sends to a client.

During the authentication session, the Enforcer sends a challenge packet to the client at a specified frequency. The default setting is every three seconds.

The Integrated Enforcer continues to send packets until one of the following conditions are met:

- The Integrated Enforcer receives a response from the client

- The Integrated Enforcer has sent the maximum number of packets specified. The default setting is 15.

The frequency (4 seconds) times the number of packets (15) is the value that is used for the Enforcer heartbeat. The heartbeat is the interval that the Integrated Enforcer allows the client to remain connected before it starts a new authentication session. The default setting is four seconds.

The client sends information to the Integrated Enforcer that contains the following items:

- Globally Unique Identifier (GUID)

- Its current Profile Serial Number

- The results of the Host Integrity check

The Integrated Enforcer verifies the client GUID and the Policy Serial Number with the Symantec Endpoint Protection Manager. If the client has been updated with the latest security policies, its Policy Serial Number matches the one that the Integrated Enforcer receives from the management server. The Host Integrity check results show whether or not the client complies with the current security policies.

After the heartbeat interval or whenever the client tries to renew its IP address, the Integrated Enforcer starts a new authentication session. The client must respond to retain the connection to the internal network.

The Integrated Enforcer disconnects the clients that do not respond.

For the clients that were previously authenticated but now fail authentication, the Integrated Enforcer updates its internal status for the client. It then sends a challenge packet to the client requesting that the client renew its IP address. When the client sends the DHCP "renew" request, the Integrated Enforcer assigns a quarantine IP address to the client.

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint Protection Manager | 1019

Configuring Symantec Network Access Control Integrated Enforcer authentication settings

Specifying the maximum number of challenge packets during an authentication session

During the authentication session, the Integrated Enforcer sends a challenge packet to the client at a specified frequency.

The Integrated Enforcer continues to send packets until the following conditions are met:

■ The Integrated Enforcer receives a response from the client

■ The Integrated Enforcer has sent the specified maximum number of packets.

The default setting is 15 for the maximum number of challenge packets for an authentication session.

To specify the maximum number of challenge packets during an authentication session

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

3 Select and expand the group of Enforcers.

The Enforcer group must include the Integrated Enforcer for which you want to specify the maximum number of challenge packets during an authentication session.

4 Under **Tasks**, click **Edit Group Properties**.

5 On the **Authentication** tab, type the maximum number of challenge packets that you want to allow during an authentication session in the **Maximum number of packets per authentication session** field.

6 In the **Settings** dialog box, on the **Authentication** tab, click **OK**.

Specifying the frequency of challenge packets to be sent to clients

During the authentication session, the Integrated Enforcer sends a challenge packet to the client at a specified frequency.

The Integrated Enforcer continues to send packets until the following conditions are met:

■ The Integrated Enforcer receives a response from the client

■ The Integrated Enforcer has sent the specified maximum number of packets.

The default setting is every 4 seconds.

1020 | Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint
Protection Manager
Configuring Symantec Network Access Control Integrated Enforcer authentication settings

To specify the frequency of challenge packets to be sent to clients

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

3 Select and expand the group of Enforcers.

The Enforcer group must include the Integrated Enforcer for which you want to specify the frequency of challenge packets to be sent to clients.

4 Under **Tasks**, click **Edit Group Properties**.

5 On the **Authentication** tab, under **Authentication Parameters**, type the maximum number of challenge packets that you want to the Integrated Enforcer to keep sending to a client during an authentication session in the **Time between packets in authentication session** field.

6 In the **Settings** dialog box, on the **Authentication** tab, click **OK**.

Allowing all clients with continued logging of non-authenticated clients

It can take some time to deploy all the client software. You can configure the Integrated Enforcer to allow all clients to connect to the network until you have finished distributing the client package to all users. These users all connect to an DHCP server at the location of this Integrated Enforcer.

The Integrated Enforcer still authenticates all users by checking that they are running a client, checking Host Integrity, and logging the results. This process occurs regardless of whether the Host Integrity checks pass or fail.

The default setting is not enabled.

Use the following guidelines when you apply the configuration settings:

■ This setting should be a temporary measure because it makes the network less secure.

■ While this setting is in effect, you can review Enforcer logs. You can learn about the types of clients that try to connect to the network at that location. For example, you can review the Client Activity Log to see if any of the clients do not have the client software installed. You can then make sure that the client software is installed on those clients before you disable this option.

To allow all clients with continued logging of non-authenticated clients

1 In the Symantec Endpoint Protection Manager Console, click **Admin**.

2 Click **Servers**.

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft DHCP Server on the Symantec Endpoint | 1021
Protection Manager
Configuring Symantec Network Access Control Integrated Enforcer authentication settings

3   Under **Servers**, select and expand the group of Enforcers.

The Enforcer group must include the Integrated Enforcer for which you want to allow all clients while continuing to log non-authenticated clients.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Settings** dialog box, on the **Authentication** tab, check **Allow all clients, but continue to log which clients are not authenticated**.

6   In the **Settings** dialog box, on the **Authentication** tab, click **OK**.

Allowing non-Windows clients to connect to a network without authentication

The Integrated Enforcer cannot authenticate a client that supports a non-Windows operating system. Therefore non-Windows clients cannot connect to the network unless you specifically allow them to connect to the network without authentication.

The default setting is not enabled.

You can use one of the following methods to enable the clients that support a non-Windows platform to connect to the network:

■   Specify each non-Windows client as a trusted host.

■   Allow all clients with non-Windows operating systems.

To allow non-Windows clients to connect to a network without authentication

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Select and expand the group of Enforcers.

The Enforcer group must include the Integrated Enforcer for which you want to allow all non-Windows clients to connect to a network.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Settings** dialog box, on the **Authentication** tab, check **Allow all clients with non-Windows operating systems**.

6   Click **OK**.

Having the Symantec Network Access Control Integrated Enforcer check the Policy Serial Number on a client

The Symantec Endpoint Protection Manager updates a client's Policy Serial Number every time that the client's security policy changes. When a client connects

to the Symantec Endpoint Protection Manager, it receives the latest security policies and the latest Policy Serial Number.

When a client tries to connect to the network through the Integrated Enforcer, the Integrated Enforcer retrieves the Policy Serial Number from the Symantec Endpoint Protection Manager. The Integrated Enforcer then compares the Policy Serial Number with the one that it receives from the client. If the Policy Serial Numbers match, the Integrated Enforcer has validated that the client is running an up-to-date security policy.

The default value for this setting is not enabled.

The following guidelines apply:

■ If the **Check the Policy Serial Number on Client before allowing Client into network** option is checked, a client must have the latest security policy before it can connect to the network through the normal DHCP server. If the client does not have the latest security policy, the client is notified to download the latest policy. The Integrated Enforcer then forwards its DHCP request to receive a quarantine network configuration.

■ If the **Check the Policy Serial Number on Client before allowing Client into network** option is not checked and the Host Integrity check is successful, a client can connect to the network. The client can connect through the normal DHCP server even if its security policy is not up to date.

To have the Symantec Network Access Control Integrated Enforcer check the Policy Serial Number on a client

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   In the **Admin** page, click **Servers**.

3   Select and expand the group of Enforcers.

    The Enforcer group must include the Integrated Enforcer that checks the Policy Serial Number on a client.

4   Under **Tasks**, click **Edit Group Properties**.

5   In the **Settings** dialog box, on the **Authentication** tab, check **Check the Policy Serial Number on the Client before allowing a Client into the network**.

6   Click **OK**.

Configuring logs for the Symantec Network Access Control Integrated Enforcer

Logs for a Symantec Network Access Control Integrated Enforcer are stored on the same computer on which you installed the Symantec Network Access Control Integrated Enforcer. Enforcer logs are generated by default.

If you want to view Enforcer logs on the Symantec Endpoint Protection Manager Console, you must enable the sending of logs on the Symantec Endpoint Protection Manager Console. If this option is enabled, the log data is sent from the Integrated Enforcer to the Symantec Endpoint Protection Manager and stored in a database.

You can modify the log settings for the Integrated Enforcer on the Symantec Endpoint Protection Manager Console. Activities are recorded in the same Enforcer Server log for all Enforcers on a site.

You can configure settings for the following logs that the Integrated Enforcer generates:

■ Enforcer Server log
The Enforcer Server log provides the information that is related to the functioning of an Enforcer.

■ Enforcer Client log
The Client log provides information about interactions between the Integrated Enforcer and the clients that have tried to connect to the network. It provides information on authentication, failed authentication, and disconnection.

Installing the Symantec Integrated Enforcer for Microsoft Network Access Protection

This chapter includes the following topics:

Before you install the Symantec Integrated Enforcer for Microsoft Network Access Protection

Before you install the Symantec Integrated Enforcer for Microsoft Network Access Protection, you must have completed the following installation and configuration tasks:

- Installation of the Symantec Endpoint Protection Manager

Note: It is recommended that you install Symantec Endpoint Protection Manager before you install the Symantec Integrated Enforcer for Network Access Protection. The Symantec Endpoint Protection Manager must be installed before the Symantec Integrated Enforcer for Microsoft Network Access Protection can work properly.

See "Installing Symantec Endpoint Protection Manager" on page 95.

- Verification of hardware and software requirements for the computer on which you plan to install the following components:

  - DHCP Server service

  - Network Access Protection Server service

  - Domain Controller

  - Symantec Integrated Enforcer for Microsoft Network Access Protection

  See "Components of a Symantec Integrated Enforcer for Microsoft Network Access Protection" on page 1029.

Process for installing the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection

Table 55-1 lists the steps to install the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection.

Table 55-1 Installation summary for the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection

Step	Action	Description
Step 1	Read the system requirements and the installation requirements.	Identifies the hardware, software, and Symantec Network Access Control components you need to obtain to run the Enforcer and plan its placement on your network. See "System requirements for an Integrated Enforcer for Microsoft Network Access Protection" on page 1027. See "Components of a Symantec Integrated Enforcer for Microsoft Network Access Protection" on page 1029.

Table 55-1   Installation summary for the Symantec Network Access Control
Integrated Enforcer for Microsoft Network Access Protection
(continued)

Step	Action	Description
Step 2	Install the Symantec Endpoint Protection Manager.	Installs the application that you use to support the Enforcer on your network. See "Installing Symantec Endpoint Protection Manager" on page 95.
Step 3	Install the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection.	Installs the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection components. See "Installing the Integrated Enforcer for Microsoft Network Access Protection" on page 1030.

System requirements for an Integrated Enforcer for Microsoft Network Access Protection

Table 55-2 summarizes the minimum requirements for the computers on which you install the Integrated Enforcer for Microsoft Network Access Protection.

Table 55-2   Integrated Enforcer for Microsoft Network Access Protection system requirements

Component	Requirement
Hardware	**Note:** Your hardware choices are affected by the type of NAP enforcement you plan to us. The following are guidelines.
	For installations of up to 10,000 users, use the following recommended requirements:
	■ Pentium III 750 MHz
	■ 256 MB of memory
	■ 120 MB of disk space
	■ Fast Ethernet network adapters
	■ One network interface card (NIC) with TCP/IP installed
	For installations of 10,000 users or greater, use the following recommended requirements:
	■ Pentium 4 2.4 GHz
	■ 512 MB of memory
	■ 512 MB of disk space
	■ 1-GB network adapters
	■ 800 x 600 resolution monitor with 256 colors (minimum)
	■ One network interface card (NIC) with TCP/IP installed

Table 55-2   Integrated Enforcer for Microsoft Network Access Protection system
requirements *(continued)*

Component	Requirement

Operating system	Ensure that the following operating system and services are installed:
	
	■ Windows Server 2008 Standard Edition
	■ Windows Server 2008 Enterprise Edition, x86 and x64 versions
	■ Windows 2008 R2
	■ You can select one of the following configurations:
	  ■ Windows Server 2008 DHCP service if you plan to use DHCP enforcement.
	    The Windows Server 2008 DHCP service should be located on the same computer as the Windows Server 2008 Network Policy Server.
	  ■ Windows DHCP service if you plan to use 802.1x enforcement.
	    The Windows DHCP service can be located on the same computer as the Windows Server 2008 Network Policy Server. You can also configure the DHCP service on a separate computer that you have configured as a Windows 2008 DHCP server or a Windows 2003 DHCP server.
	■ Windows Server 2008 Network Policy Server (NPS) service

Components of a Symantec Integrated Enforcer for Microsoft Network Access Protection

The Symantec Integrated Enforcer for Microsoft Network Access Protection works with the Microsoft DHCP Server, the Symantec Endpoint Protection Manager, and the Symantec Network Access Control client with Network Access Protection enabled. The Symantec Integrated Enforcer for Microsoft Network Access Protection verifies that the clients comply with configured security policies before any clients can connect to a network.

The following required components must be installed before you can use the Symantec Integrated Enforcer for Network Access Protection:

Symantec Endpoint Protection Manager version 12.1	Required to create security policies in a centralized location and assign them to clients.

Windows 2008 server DHCP Server service as well as the Network Policy Server (NPS) service must also be installed on the same computer	Required installation of the Microsoft Windows Server with the DHCP Server service and the Network Policy Server service. These two services must be installed and configured before you can install the Symantec Network Access Protection Integrated Enforcer.
Domain Controller	Required installation of the Domain Controller on the same computer as the Symantec Endpoint Protection Manager or on a different computer that supports Microsoft Windows Server 2003.
Symantec Integrated Enforcer for Microsoft Network Access Protection	Required to authenticate clients and enforce security policies.
Symantec Network Access Control client	Required installation of the Symantec Network Access Control client.

Installing the Integrated Enforcer for Microsoft Network Access Protection

You must install the Integrated Enforcer for Microsoft Network Access Protection on the same computer on which you have already installed the Microsoft Network Policy Server. You must log in as an administrator or a user in the administrators group.

Note: After you complete the installation of the Symantec Integrated NAP Enforcer, you must connect to the Symantec Endpoint Protection Manager.

To install the Integrated Enforcer for Microsoft Network Access Protection with the Installation Wizard

1   Insert the product disc for Symantec Network Access Control into the DVD drive to start the installation automatically.

   If the installation does not start automatically, double-click one of::

   ■   **IntegratedEnforcerInstaller86.exe** (for x86 OSes).

   ■   **IntegratedEnforcerInstaller64.exe** (for x64 OSes).

   You must exit the installation and install the NPS server if the NPS server is not already installed.

If the NAP Server service is already installed, the **Welcome to Symantec Integrated NAP Enforcer Installation Wizard** appears.

2   In the **Welcome** panel, click **Next**.

3   In the **License Agreement** panel, click **I accept the license agreement**.

4   Click **Next**.

5   In the **Destination Folder** panel, perform one of the following tasks:

   ■   If you want to accept the default destination folder, click **Next**.
       The install location defaults to one of:

      ■   `C:\Program Files\Symantec\Symantec Endpoint Protection\Integrated Enforcer` for x86 OSes.

      ■   `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Integrated Enforcer` for x64 OSes.

   ■   Click **Browse** to locate and select a destination folder, click **OK**, and click **Next**.

6   If the **Role Selection** panel appears, select **NAP Enforcement** and click **Next**.

    The **Role Selection** panel only appears if more than one type of Symantec NAC Integrated Enforcer can be installed based on the services running on the server.

7   In the **Ready to Install the Application** panel, click **Next**.

    If you need to modify any of the previous settings, click **Back**.

8   Click **Finish**.

    If you need to reinstall the Symantec Integrated NAP Enforcer, you must first uninstall it.

9   Click **Start > Programs > Symantec Endpoint Protection Manager > Symantec NAC Integrated Enforcer**.

Uninstalling the Integrated Enforcer for Microsoft Network Access Protection

You can uninstall the Integrated Enforcer for Microsoft Network Access Protection from the Windows taskbar or the command line.

To uninstall the Integrated Enforcer for Microsoft Network Access Protection

1   On the Windows taskbar, click **Start > Control Panel > Add or Remove Programs**.

2   Click **Symantec NAC Integrated Enforcer,** and then click **Remove**.

3 To respond the prompt about whether you want to remove the software, click **Yes**.

4 To respond the prompt about whether you want to restart the NPS server, do one of the following:

- To restart the NPS server immediately, click **Yes**.

- To restart the NPS service manually later (the default), click **No**.
  If you restart the NPS service later, you must stop and then start it.
  You must restart the NPS service to completely uninstall the Symantec Integrated Enforcer.

To uninstall the Integrated Enforcer for Microsoft Network Access Protection from the command line

1 Open a DOS command window.

2 At the command prompt, type one of:

- `MsiExec.exe /qn/X{A145EB45-0852-4E18-A9DC-9983A6AF2329}` for x86

- `MsiExec.exe /qn/X{977BF644-A8FF-484f-8AF7-C1AF40F38DEA}` for x64

3 Restart the NPS server.

Stopping and starting the Network Access Protection server manually

Stop the Network Access Protection (NAP) server manually before upgrading to a new version of the Integrated Enforcer for Microsoft Network Access Control. You then restart it after you complete the upgrade.

To stop and start the NAP server manually

1 On the Windows taskbar, click **Start > Control Panel > Administrative Tools > Services**.

2 Click **NAP Server**.

3 Right-click, and then click **Stop**.

4 Click **Start**.

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console

This chapter includes the following topics:

- About configuring a Symantec Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console

- Connecting a Symantec Integrated Enforcer for Microsoft Network Access Protection to a management server on an Enforcer console

- Encrypting communication between a Symantec Integrated Enforcer for Microsoft Network Access Protection and a management server

- Setting up an Enforcer group name on the Symantec Integrated Enforcer for Microsoft Network Access Protection console

- Setting up an HTTP communication protocol on the Symantec Integrated Enforcer for Microsoft Network Access Protection console

About configuring a Symantec Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console

After you complete the installation of the Symantec Integrated NAP Enforcer, you must perform the following tasks before the Symantec Integrated Enforcer for Microsoft Network Access Protection can become operational.

Table 56-1   Enforcer console configuration summary

Step	Action	Description
Step 1	Connect the Integrated Enforcer to a Symantec Endpoint Protection Manager.	Specify the Symantec Endpoint Protection Manager to which the Symantec Integrated Enforcer for Microsoft Network Access Protection can connect.
		You include the host name or IP address of the Symantec Endpoint Protection Manager in a file that is called a management server list. The Symantec NAC Integrated Enforcer must connect to an IP address or host name of a Symantec Endpoint Protection Manager. Otherwise the configuration fails.
		See "Connecting a Symantec Integrated Enforcer for Microsoft Network Access Protection to a management server on an Enforcer console" on page 1035.
Step 2	Encrypt communication between the Integrated Enforcer and the management server.	Add an encrypted password or a preshared secret that you configured during the installation of the Symantec Endpoint Protection Manager.
		The encrypted password was previously known as a preshared key.
		See "Encrypting communication between a Symantec Integrated Enforcer for Microsoft Network Access Protection and a management server" on page 1037.
Step 3	Name the Enforcer group.	Set up an Enforcer group name
		See "Setting up an Enforcer group name on the Symantec Integrated Enforcer for Microsoft Network Access Protection console" on page 1038.

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection on an Enforcer console | 1035

Connecting a Symantec Integrated Enforcer for Microsoft Network Access Protection to a management server on an Enforcer console

	Table 56-1	Enforcer console configuration summary *(continued)*

Step	Action	Description
Step 4	Set up an HTTP or HTTPS communication protocol.	Establish HTTP or HTTPS communication between the Symantec Integrated Enforcer for Microsoft Network Access Protection and the Symantec Endpoint Protection Manager. See "Setting up an HTTP communication protocol on the Symantec Integrated Enforcer for Microsoft Network Access Protection console" on page 1039.

Connecting a Symantec Integrated Enforcer for Microsoft Network Access Protection to a management server on an Enforcer console

You need to connect a Symantec Integrated Enforcer for Microsoft Network Access Protection (NAP Enforcer) to a management server on a Network Access Protection Enforcer console.

To establish communication between the Integrated Enforcer console and Symantec Endpoint Protection Manager

1   On the Windows taskbar of the Integrated Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer**.

    The Symantec Network Access Control Integrated Enforcer configuration console appears. This main page shows the connection status between the Integrated Enforcer and the Symantec Endpoint Protection Manager. A green light indicates that Integrated Enforcer is actively connected to the management server. A red light indicates that the connection is disconnected.

2   In the left-hand panel, click **Symantec Integrated Enforcer > Configure > Management Server**.

3   In the **Management Server** dialog box, type the IP address or name of the Symantec Endpoint Protection Manager in the **Server address** text field.

    You can type an IP address, host name, or domain name. If you want to use a host name or a domain name, ensure that the name resolves correctly with the Domain Name Server (DNS server).

4   In the **Management Server** dialog box, edit the port number that the Integrated Enforcer uses to communicate with the Symantec Endpoint Protection Manager.

The default port number is 8014 for HTTP protocol and 443 for the HTTPS protocol. You can only use the HTTPS protocol if it is configured in the same way on the Symantec Endpoint Protection Manager.

5   In the **Encryption password** text box, type the password of the Symantec Endpoint Protection Manager for your connection.

The Symantec Endpoint Protection Manager and Integrated Enforcer must use the same encrypted password for communication.

To display the letters and numbers of the preshared key instead of asterisks, check **Use Hash Value**. If **Use Hash Value** is turned on, the encryption password must be 32 characters, and must use hexadecimal numbers only.

6   In the **Preferred** group text box, type a name for the Integrated Enforcer group.

If you do not specify a group name, the Symantec Endpoint Protection Manager assigns the Symantec Network Access Control Integrated Enforcer to a default Enforcer group with default settings. The default group name is I-DHCP. However, a Symantec Network Access Control Integrated Enforcer for Microsoft NAP Servers and appliance-based enforcers must each be in a separate group.

You can view the group settings from the Symantec Endpoint Protection Manager console on the **Servers** page.

7   To specify the protocol that the Symantec Network Access Control Integrated Enforcer uses to communicate with the Symantec Endpoint Protection Manager, select **HTTP** or **HTTPS**.

You can only use the HTTPS protocol if the Symantec Endpoint Protection Manager is running Secure Sockets Layer (SSL).

If you select HTTPS and want to require verification of the management server's certificate with a trusted third-party certificate authority, check **Verify certificate when using HTTPs protocol**.

8   Click **Save**.

After the Integrated Enforcer connects to the Symantec Endpoint Protection Manager, you can change most of the configuration settings on the Symantec Endpoint Protection Manager Console. However, the preshared secret or encrypted password must be the same on the Integrated Enforcer and the Symantec Endpoint Protection Manager in order for them to communicate.

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection on an | 1037
Enforcer console
Encrypting communication between a Symantec Integrated Enforcer for Microsoft Network Access Protection and a
management server

To remove a Symantec Endpoint Protection Manager from a management server list on a Symantec Integrated NAP Enforcer console

1   On the Windows taskbar of the Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec Integrated NAP Enforcer**.

2   In the left-hand panel, expand Symantec NAP Enforcer.

3   Expand Configure.

4   Click **Management Servers**.

5   To remove a Symantec Endpoint Protection Manager, click **Remove** or **Remove All** from the icon column.

Encrypting communication between a Symantec Integrated Enforcer for Microsoft Network Access Protection and a management server

If you want to add another layer of security, you can secure communication between the Symantec NAC Integrated Enforcer and the Symantec Endpoint Protection Manager through encryption. Encrypted communication requires the use of the HTTPS protocol instead of the HTTP protocol. You also need to purchase a third-party certificate from a vendor.

You typically configure an encrypted password during the installation of the Symantec Endpoint Protection Manager for the first time. The same password must be configured on the Symantec Integrated NAP Enforcer. If the encrypted passwords do not match, communication between the Symantec Integrated NAP Enforcer and the Symantec Endpoint Protection Manager fails.

To encrypt communication between a Symantec NAC Integrated Enforcer and a management server

1   On the Windows taskbar of the Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec Integrated NAP Enforcer**.

2   In the left-hand panel, expand Symantec NAP Enforcer.

3   Expand Configure.

4   Click **Management Servers**.

1038 | Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection on an
Enforcer console
Setting up an Enforcer group name on the Symantec Integrated Enforcer for Microsoft Network Access Protection
console

5   Type the encrypted password in the Encrypted Password text box on the Symantec Integrated NAP Enforcer console.

The Symantec Integrated NAP Enforcer must use the same encrypted password for communication with the Symantec Endpoint Protection Manager. The encrypted password is always configured during the installation of the Symantec Endpoint Protection Manager.

6   Check **Use Hash Value**. If **Use Hash Value** is checked, the encryption password must be 32 characters and must use hexadecimal numbers only.

The letters and numbers of the encrypted password now appear instead of asterisks.

7   Click **OK**.

Setting up an Enforcer group name on the Symantec Integrated Enforcer for Microsoft Network Access Protection console

You must add a name for the Enforcer group. After the Symantec NAC Integrated Enforcer connects to a Symantec Endpoint Protection Manager, it registers the name of the Enforcer group automatically on the management server.

To set up an Enforcer group name on the Symantec NAC Integrated Enforcer console

1   On the Windows taskbar of the Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec Integrated NAP Enforcer**.

2   In the left-hand panel, expand Symantec NAP Enforcer.

3   Expand Configure.

4   Click **Management Servers**.

5   In the right-hand panel, type the name of the Enforcer group in the Preferred group text box on the Symantec Integrated NAP Enforcer console.

If you do not add a name for the Integrated Enforcer group on the Enforcer console, then all Integrated Enforcers automatically become part of the Temporary group on the management server. If you add the name of the Integrated Enforcer group on the Enforcer console, then the name of the Enforcer group is automatically registered on the management server.

6   Click **OK**.

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection on an | 1039
Enforcer console
Setting up an HTTP communication protocol on the Symantec Integrated Enforcer for Microsoft Network Access
Protection console

Setting up an HTTP communication protocol on the Symantec Integrated Enforcer for Microsoft Network Access Protection console

You need to establish a communication protocol between the Symantec Integrated Enforcer for Microsoft Network Access Protection and the Symantec Endpoint Protection Manager. Otherwise the communication between the Symantec Integrated Enforcer for Microsoft Network Access Protection and the Symantec Endpoint Protection Manager fails.

You can set up a HTTP or HTTPS protocol. If you select the HTTPS protocol, you need to purchase a certificate from a third-party vendor.

To set up an HTTP communication protocol on the Symantec Integrated Enforcer for Microsoft Network Access Protection

1 On the Windows taskbar of the Enforcer computer, click **Start > Programs > Symantec Endpoint Protection > Symantec NAC Integrated Enforcer**.

2 In the left-hand panel, expand Symantec NAP Enforcer.

3 Expand Configure.

4 Click **Management Servers**.

5 In the right-hand panel of the Symantec Integrated NAP Enforcer console, click HTTP.

   If you want to set up encrypted communication between the Symantec Integrated NAP Enforcer and the Symantec Endpoint Protection Manager, you must use the HTTPS protocol.

6 If you need to verify the certificate because you use the HTTPS protocol, check **Verify certificate when using HTTPS protocol**.

7 Click **OK**.

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection on the Symantec Endpoint Protection Manager

This chapter includes the following topics:

- About configuring the Symantec Integrated Enforcer for Microsoft Network Access Protection on the Symantec Endpoint Protection Manager

- Enabling NAP enforcement for clients

- Verifying that the management server manages the client

- Verifying Security Health Validator policies

- Verifying that clients pass the Host Integrity check

- Configuring logs for the Symantec Integrated Enforcer for Network Access Protection

About configuring the Symantec Integrated Enforcer for Microsoft Network Access Protection on the Symantec Endpoint Protection Manager

If you want to support the Symantec Integrated Enforcer for Microsoft Network Access Protection in a network environment, you must enable NAP enforcement on the Symantec Endpoint Protection Manager. Otherwise the Enforcer works incorrectly.

You also need to define one or more criteria for the Security Health Validator policy requirements. For example, you can verify whether or not the client's Security Health Validator policy is the latest one that has been installed on a client. If it is not the latest Security Health Validator policy, then the client is blocked and is therefore unable to connect to the network.

Table 57-1   Symantec Endpoint Protection Manager configuration summary

Step	Action	Description
Step 1	Enable Network Access Protection enforcement for clients.	Enable Network Access Protection enforcement for clients so that the Integrated Enforcer can run Security Health Validator policies. See "Enabling NAP enforcement for clients" on page 1043.
Step 2	Optionally, verify that the Symantec Endpoint Protection Manager is managing the Symantec Network Access Control client or the Symantec Endpoint Protection client.	Set up a verification check to ensure that the management server manages the Symantec Network Access Control client or the Symantec Endpoint Protection client. See "Verifying that the management server manages the client" on page 1044.
Step 3	Optionally, verify that the latest Security Health Validator polices are installed.	Verify that the Symantec Network Access Control client and the Symantec Endpoint Protection client have the latest Security Health Validator policies are installed See "Verifying Security Health Validator policies" on page 1044.

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection on the Symantec Endpoint Protection Manager

Enabling NAP enforcement for clients

1043

	Table 57-1	Symantec Endpoint Protection Manager configuration summary *(continued)*

Step	Action	Description
Step 4	Optionally, verify that clients pass the Host Integrity check.	Verify that clients are in compliance with the Host Integrity policy. See "Verifying that clients pass the Host Integrity check" on page 1045.
Step 5	Optionally, configure logs for viewing on the Symantec Endpoint Protection Manager.	Enable the sending of log data to the Symantec Endpoint Protection Manager. See "Configuring logs for the Symantec Integrated Enforcer for Network Access Protection" on page 1045.

Enabling NAP enforcement for clients

You must enable NAP (Network Access Protection) enforcement for Symantec Endpoint Protection and Symantec Network Access Control clients. If you do not enable NAP enforcement for clients, the Symantec Integrated Enforcer for Microsoft Network Access Protection cannot implement any Security Health Validator policies.

To enable NAP enforcement for clients

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

2   In the **Clients** page, under **View Groups**, select the group for which you want to enable NAP enforcement.

3   On the **Policies** tab, click **General Settings**.

4   In the **Settings** dialog box, click **Security Settings**.

5   On the **Security Setting**s tab, in the **Enforce Client** area, check **Enable NAP Enforcement**.

    The **Enable NAP Enforcement** setting is disabled by default.

6   Click **OK**.

1044 | Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection on the
Symantec Endpoint Protection Manager
Verifying that the management server manages the client

Verifying that the management server manages the client

You can set up a verification check to ensure that the Symantec Endpoint Protection Manager manages the Symantec Endpoint Protection client or the Symantec Network Access Control client.

To verify that the management server manages the client

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **View**, select the Enforcer group for which you want to verify that the management server manages the client.

4   Right-click the Enforcer group and select **Edit Properties**.

5   In the **Client Information area on the NAP Setting** tab in the **I-DHCP Settings** dialog box, check **Verify that the management server manages the client**.

    The **Verify that the management server manages the client** setting is disabled by default.

6   Click **OK**.

Verifying Security Health Validator policies

You can make sure that the Symantec Endpoint Protection and Symantec Network Access Control clients have the latest Security Health Validator policies installed.

To verify Security Health Validator policies

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **View,** select the group for which you want to set up Security Health Validator policies.

4   Right-click the Enforcer group and select **Edit Properties**.

5   In the **Client Information** area on the NAP Setting tab in the **I-DHCP Settings** dialog box, check **Verify that the Security Health Validator policy is current**.

    The **Verify that the Security Health Validator policy is current** setting is disabled by default.

6   Click **OK**.

Configuring the Symantec Network Access Control Integrated Enforcer for Microsoft Network Access Protection on the | 1045
Symantec Endpoint Protection Manager
Verifying that clients pass the Host Integrity check

Verifying that clients pass the Host Integrity check

You can set up a compliance check for clients on the Symantec Endpoint Protection Manager.

To verify that clients pass the Host Integrity check

1   In the Symantec Endpoint Protection Manager Console, click **Admin**.

2   Click **Servers**.

3   Under **View**, select the Enforcer group for which you want to verify that the client has passed the Host Integrity check.

4   Right-click the Enforcer group and select **Edit Properties**.

5   In the **Host Integrity Status** area on the **NAP Setting** tab in the **I-DHCP Settings** dialog box, check **Verify that the client passes the Host Integrity check**.

    The **Verify that the client passes the Host Integrity check setting** is disabled by default.

6   Click **OK**.

Configuring logs for the Symantec Integrated Enforcer for Network Access Protection

Logs for the Symantec Integrated Network Access Protection (NAP) Enforcer are stored on the same computer on which you installed the Symantec Integrated NAP Enforcer. Enforcer logs are generated by default.

If you want to view Enforcer logs on the Symantec Endpoint Protection Manager Console, you must enable the sending of logs on the Symantec Endpoint Protection Manager Console. If this option is enabled, the log data is sent from the Symantec Integrated NAP Enforcer to the Symantec Endpoint Protection Manager and stored in a database.

You can modify the log settings for the Symantec Integrated NAP Enforcer on the Symantec Endpoint Protection Manager Console. Activities are recorded in the same Enforcer Server log for all Enforcers on a site.

You can configure settings for the following logs that the Symantec Integrated NAP Enforcer generates:

■   Enforcer Server log
    The Enforcer Server log provides the information that is related to the functioning of an Enforcer.

■ Enforcer Client log
The Client log provides information about interactions between the Integrated Enforcer and the clients that have tried to connect to the network. It provides information on authentication, failed authentication, and disconnection.

Setting up temporary connections for Symantec Network Access Control On-Demand clients

This chapter includes the following topics:

About the Symantec Network Access Control On-Demand Clients

End users often need to temporarily connect to an enterprise network even though their computers do not have the approved software. If an enterprise network includes a Gateway Enforcer appliance, the Enforcer can install On-Demand clients on computers so that they are compliant. Once the Enforcer has installed an On-Demand client, it temporarily connects to an enterprise network as a guest.

The administrator can configure a Gateway Enforcer appliance to automatically download Symantec Network Access Control On-Demand clients on both Windows and Mac platforms. As soon as the Symantec Network Access Control On-Demand client is downloaded to a client computer, the client can try to connect to the company's network.

See "What you can do with On-Demand Clients" on page 795.

See "How the On-Demand Client works" on page 792.

Before you configure Symantec Network Access Control On-Demand clients on the console of a Gateway Enforcer

Before you can set up the automatic downloading of the Symantec Network Access Control On-Demand clients for Windows and Macintosh, you must have already completed the following tasks:

- Installed the Symantec Network Access Control software that is located on the product disc. This software includes the Symantec Endpoint Protection Manager software that you must install.

- Written down the name of the encrypted password that you implemented during the installation of the Network Access Control software.

- Installed and configured a Gateway Enforcer appliance.
  When you install and configure an Enforcer appliance for the first time, it assigns a name to the Enforcer group during the installation process. You must plan the assignment of IP addresses, host names, as well as the configuration of the network interface cards (NICs). If the NICs are incorrectly configured, then the installation fails or behaves in unexpected ways.
  The name of the Enforcer group automatically appears on the console of the Symantec Endpoint Protection Manager in the **Server** pane that is associated with each Enforcer appliance.
  You can also set up guest access with the DHCP Integrated Enforcer.

See "Setting up guest access challenge using the Symantec Network Access Control DHCP Integrated Enforcer" on page 1050.

■ Checked the connection status between the Enforcer appliance and the management server on the console of the Enforcer appliance.
See "Checking the communication status of an Enforcer appliance on the Enforcer console" on page 854.
See "About the Enforcer appliance CLI command hierarchy" on page 855.

■ Enabled an HTTP redirect or DNS spoofing on the console of the Symantec Endpoint Protection Manager.
The HTTP redirect or DNS spoofing is the IP address of the internal NIC (eth0) that is located on a Gateway Enforcer appliance.
See "Redirecting HTTP requests to a Web page" on page 891.
For HTTP redirect, you add the URL in the Admin page on the Symantec Endpoint Protection Manager. After you display the **Admin** page, you must display the Servers pane and select the Enforcer group under **View Servers**. If you select the Enforcer group of which the Gateway Enforcer is a member, click **Edit Group Properties** under **Tasks**. In the **Enforcer Settings** dialog box, you select the **Authentication** tab and type the URL in the HTTP redirect URL field.

■ You must create the client group as a subgroup of the My Company group with Full Access rights.
You add the client group on the Clients page as a subgroup of the My Company group on the Symantec Endpoint Protection Manager.
Make sure that you write down the name of the Enforcer client group that manages Symantec Network Access Control On-Demand clients. If you do not create a separate group, then the Default group on the Symantec Endpoint Protection Manager takes over the management of the Symantec Network Access Control On-Demand clients.

■ Created an optional separate location for an Enforcer client group on the Symantec Endpoint Protection Manager Console.
If you do not create a separate location for the group that manages the Symantec Network Access Control On-Demand or guest clients, then the default location is automatically assigned to the guest clients. The best practice is to create a separate location for the Enforcer client group on the Symantec Endpoint Protection Manager. Another best practice is to use different groups for Windows and Mac clients. Their capabilities differ. For example, Windows on-demand clients can be configured to have pop-up messages. Mac clients cannot.
Location criteria help you define the criteria that can identify Symantec Network Access Control On-Demand or guest clients by its IP address, MAC address, host name, or other criteria. The best practice is to create a separate

location to which all Symantec Network Access Control On-Demand or guest clients are automatically assigned if they want to connect to a network on a temporary basis without the correct credential.

You can add and assign a location to the Enforcer client group in the **Clients** page, under **Tasks**, on the Symantec Endpoint Protection Manager.

■ Added and assigned an optional Host Integrity policy to the Enforcer client group and location on the Symantec Endpoint Protection Manager Console.

It is optional to add and assign a Host Integrity policy to the Enforcer client group and location on the console of a Symantec Endpoint Protection Manager, but the best practice to specify the following criteria:

  ■ How frequently a host integrity check is run

  ■ Type of Host Integrity policy that you want to implement

You can add and assign an optional Host Integrity policy to an Enforcer client group and location in the **Policies** page, under **Tasks**, on the Symantec Endpoint Protection Manager.

■ Enabled an optional pop-up message for Windows clients. You configure this on the Symantec Endpoint Protection Manager Console.

■ Obtain the domain ID number that is located on the Symantec Endpoint Protection Manager Console.

You should have the domain ID handy because you may need to configure the domain ID on the Gateway or DHCP Enforcer with the on-demand spm-domain command.

Setting up guest access challenge using the Symantec Network Access Control DHCP Integrated Enforcer

Guest Access and the DHCP Integrated Enforcer require a Gateway Enforcer and DNS server, because the DHCP Integrated Enforcer does not support DNS spoofing.

The first step towards enabling this solution is to set up a separate DNS server and Gateway Enforcer in the quarantine network. The guest endpoint receives a restricted and quarantined IP address with this DNS server. This quarantine DNS server resolves all DNS request to the Gateway Enforcer. The guest endpoint receiving the DNS resolution sends all HTTP request to the Gateway Enforcer. The Gateway Enforcer which then redirects the request to the on-demand Web server for download of the on-demand client. Once the download to the endpoint completes, Host Integrity checking runs and the result of this (configurable policy) outcome determines access for the endpoint. If the Host Integrity check passes,

the endpoint is granted a normal IP address with the normal DNS server. If Host Integrity fails, the endpoint remains with a quarantined IP address with the quarantined DNS server.

Figure 58-1   Network diagram of DHCP Integrated Enforcer configured to prevent DNS spoofing

Normal Network
IP address: 192.168.100.22
Subnet mask:
255.255.255.0
DNS/WINS: 192.168.100.1

Guest

Quarantine Network
IP address: 192.168.100.22
Subnet mask:
255.255.255.255
DNS/WINS: 192.168.100.3

Normal DHCP/DNS/WINS
(Win2k3)
DHCP Integrated Enforcer installed
192.168.100.1

SEPM (Win2k3)
192.168.100.2

Quarantine DNS/WINS
(Win2k3)
102.168.100.3

Gateway Enforcer
Eth0: 192.168.100.4
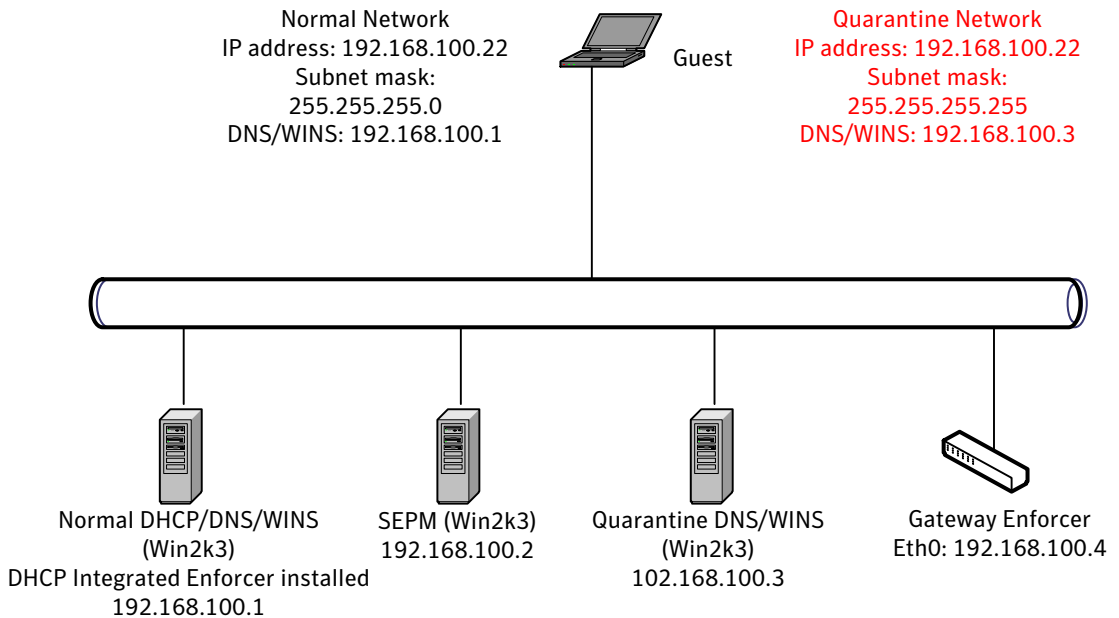
To configure the DHCP Integrated Enforcer

1   Configure the DHCP Integrated Enforcer to connect to your Symantec Endpoint Protection Manager.

2   Set up the DHCP Integrated Enforcer to use a secure subnet mask for quarantine IP addresses.

    See "Configuring a secure subnet mask" on page 1007.

3   Configure the DHCP Integrated Enforcer to add static routes to quarantine IP addresses in the DHCP server. Static routes include DHCP server (192.168.100.1), DNS server (192.168.100.3), SEPM server (192.168.100.2), and Gateway Enforcer internal IP address (192.168.100.4)

4   Verify that static routes are added in the DHCP server. This is configured on the Enforcer console: click **Scope options** and ensure that **033 Static Route Option** is checked for each route.

5   Add a DNS server. Right click on **Scope options**, and then click **Configure options...**.

6   On the **Advanced** tab, select **DHCP Standard Options** as the **Vendor class** and **Default User Class** as the **User class**.

7   In the **Available Options** scrolling box, click to select **006 DNS Servers**.

8   In the **IP address** fill-in box, add the normal DNS server IP address (**192.168.100.1**).

9   Click **Apply**.

10 Add a WINS server, using your usual procedures.

11 Configure quarantine IP address scope settings.

12 Right click on **Scope options**, and then click **Configure options...**.

13 On the **Advanced** tab, select **DHCP Standard Options** as the **Vendor class** and **SNAC_QUARANTINE** as the **User class**.

14 In the **Available Options** scrolling box, click to select **006 DNS Servers**.

15 In the **IP address** fill-in box, add the quarantine DNS server IP address (**192.168.100.3**).

16 Click **Apply**.

17 Add a quarantine WINS server, with the quarantine address of **192.168.100.3**.

18 Click **Apply**.

Next you set up the Gateway Enforcer.

To configure the Gateway Enforcer as a guest appliance

1   Connect **eth0** to the network and set the IP address to **192.168.100.4**.

2   Disconnect **eth1**.

3   Configure settings for configuration of Symantec Endpoint Protection Manager, using the command-line interface on the Gateway Enforcer:

```
configure
spm ip 192.168.100.2 key sygate group Gateway
```

4   Ensure that the Enforcer is connected to Symantec Endpoint Protection Manager, by issuing the `show status` command.

5   Enable on-demand, using the command-line interface:

```
On-demand
Spm-domain name <domain name>
Client-group <client group full path>
Enable
Show
```

Next you set up a quarantine Windows DNS setup for HTTP redirect.

To set up a quarantine Windows DNS HTTP redirect

1   Open the DNS management console on the quarantine DNS server (192.168.100.3).

2   Right click **Forward Lookup Zones** and select **New Zone**. The **New Zone Wizard** appears.

3   In the **New Zone Wizard**, click **Next**.

4   Select **Primary zone**, and click **Next**.

5   Type a period (.) as the **Zone name**, and click **Next**.

6   Select **Create a new file with this file name**, type **root.dns**, and click **Next**.

7   Select **Do not allow dynamic updates**, and click **Next**.

8   Click **Finish**.

Create a new host under the **.(root)** zone that you just created.

To create a new host in the .(root) zone

1   Right click on the **.(root)** zone, and then select **New Host**.

2   Type an asterisk (*) as the **Name** and the Gateway Enforcer IP address (**192.168.100.4**) as the IP address for the new host.

3   Click **Add Host**.

Change the lookup IP address of the DNS server itself.

To change the IP address of the DNS server

1   Double click the DNS server name in the right panel.

2   Change the IP address to the Enforcer IP address (**192.168.100.4**), and click **OK**.

Optional: You may want to set up the WINS server to resolve in the same fashion as the DNS server. Computer names are resolved by the WINS server. If the

endpoint is not registered to a domain, it resolves its computer name through WINS server. You may choose to set up a separate WINS server in quarantine to resolve all computer names in the internal network to the Gateway Enforcer **eth0** (**192.168.100.4**).

You should test your configuration.

To test your configuration

1   On the command prompt on the client computer, type

```
ipconfig /release
ipconfig /renew
```

The client should get a quarantine IP address with `255.255.255.255` as the subnet mask, and `192.168.100.3` as the DNS server

2   Clear the DNS cache. Type **ipconfig /flushdns**

3   Open a Web browser and type **www.yahoo.com**.

You should be redirected to the Gateway Enforcer on-demand Web site.

4   Download the on-demand client , and pass Host Integrity checks.

5   Your client is issued a normal IP address and `192.168.100.1` as the DNS server.

Enabling Symantec Network Access Control On-Demand clients to temporarily connect to a network

If you want to enable the automatic downloading of a Symantec Network Access Control On-Demand client on a client computer on the Windows and Macintosh platforms, you must have already completed a number of configuration tasks.

See "Before you configure Symantec Network Access Control On-Demand clients on the console of a Gateway Enforcer" on page 1048.

You need to configure the following commands before you can enable Symantec Network Access Control On-Demand clients to connect to a network:

■ Execute the `spm-domain` command.

■ Execute the `client-group` command.

■ Execute the `enable` command.

■ Execute the `authentication enable` command. This command is optional.

To enable Symantec Network Access Control On-Demand clients to temporarily connect to a network

1   Log on to the Gateway Enforcer appliance console as a superuser.

    See "Logging on to an Enforcer appliance" on page 804.

2   On the console of a Gateway Enforcer appliance, type the following command:

    Enforcer #on-demand

3   Type the following command:

    Enforcer (on-demand)# spm-domain

    where:

    spm-domain represents a string that is displayed in the Enforcer automatically.

    See "Before you configure Symantec Network Access Control On-Demand clients on the console of a Gateway Enforcer" on page 1048.

4   Type the following command:

    Enforcer (on-demand)# client-group "My Company/*name of Enforcer client group*"

    where:

    name of Enforcer client group represents the name of the Enforcer client group that you already set up in the Clients page under View Clients on the console of a Symantec Endpoint Protection Manager. You should have already set up this Enforcer client group as a subgroup to the My Company group with full access rights. If you have not set the Enforcer client group on the console of a Symantec Endpoint Protection Manager, the Enforcer registers to the Default group. The information about the Enforcer client group is automatically sent during the next heartbeat.

    You can now set up authentication for the Symantec Network Access Control On-Demand clients.

    See "Setting up authentication on the Gateway Enforcer console for Symantec Network Access Control On-Demand clients" on page 1056.

5   Type the following command:

    Enforcer (on-demand)#enable

You can also set the duration of time that the on-demand client will be "live," using the persistence command.

To make the Symantec Network Access Control On-Demand clients "persistent"

1   Log on to the Gateway Enforcer appliance console as a superuser.

    See "Logging on to an Enforcer appliance" on page 804.

2   On the console of a Gateway Enforcer appliance, type the following command:

    Enforcer #`on-demand`

3   Type the following command

    Enforcer (on-demand)# `persistence duration days 10`

    where:

    `duration days 10` indicates that you want the client to persist for 10 days.

Disabling Symantec Network Access Control On-Demand clients

If you want to stop allowing guest access, you can disable it.

To disable Symantec Network Access Control On-Demand clients for client computers

1   Log on to the Gateway Enforcer appliance console as superuser.

    See "Logging on to an Enforcer appliance" on page 804.

2   On the console of a Gateway Enforcer appliance, type `on-demand`.

3   Type `disable`.

4   Type `exit`.

5   Type `exit` to log off.

Setting up authentication on the Gateway Enforcer console for Symantec Network Access Control On-Demand clients

You can authenticate end users with On-Demand clients by enabling one of the following for authentication.

■ The local database of the Gateway Enforcer appliance.
   See "Setting up user authentication with a local database" on page 1057.

■ A Microsoft Windows Server 2003 Active Directory configured to manage the authentication of the end users with the Gateway Enforcer appliance.
See "Setting up user authentication with a Microsoft Windows 2003 Server Active Directory" on page 1057.

■ A RADIUS server configured to manage the authentication of the end users with the Gateway Enforcer appliance.
See "Setting up user authentication with a RADIUS server" on page 1058.

Once you enable authentication, add user names and a password for each authenticated end user.

Setting up user authentication with a local database

You can configure up to 1,000 users in the local on-board database of the Gateway Enforcer appliance.

See "on-demand authentication local-db commands" on page 1066.

To set up authentication with a local database

1   Log on to the Gateway Enforcer appliance console as a superuser.

See "Logging on to an Enforcer appliance" on page 804.

2   On a Gateway Enforcer appliance console, type the following command:

```
Enforcer # on-demand
```

3   On a Gateway Enforcer appliance console, type the following command:

```
Enforcer (on-demand)# authentication
```

4   Type the following command:

```
Enforcer (authentication)# local-db add user name username
password password
```

5   Type the following command:

```
Enforcer (authentication)# local-db enable
```

6   Type the following command:

```
Enforcer (authentication)# enable
```

Setting up user authentication with a Microsoft Windows 2003 Server Active Directory

The Gateway Enforcer appliance establishes a connection to the Microsoft Windows 2003 Server through the domain name instead of the IP address. Therefore you

must have set up a Domain Name Server (DNS) in the network that can resolve the domain name.

See "on-demand authentication ad commands" on page 1063.

To set up authentication with an Active Directory server

1   Log on to the Gateway Enforcer appliance console as a superuser.

    See "Logging on to an Enforcer appliance" on page 804.

2   On a Gateway Enforcer appliance console, type the following command:

    Enforcer #`on-demand`

3   Type the following command:

    Enforcer (on-demand)# `authentication`

4   Type the following command:

    Enforcer (authentication)# `ad domain` *domain* `name` *alias name*

5   Type the following command:

    Enforcer (authentication)# `ad enable`

6   Type the following command:

    Enforcer (authentication)# `enable`

Setting up user authentication with a RADIUS server

You can set up and configure one or more RADIUS servers for authentication. For example, you might want to have multiple RADIUS servers for load balancing.

See "on-demand authentication RADIUS server commands" on page 1065.

Note: Note that certificates need to be imported to the Enforcer for PEAP and TLS clients.

To set up the On-Demand client for authentication with a RADIUS server

1   Log on to the Gateway Enforcer appliance console as a superuser.

    See "Logging on to an Enforcer appliance" on page 804.

2   Type the following command:

    ```
    Enforcer# on-demand
    ```

3   Type the following command:

    ```
    Enforcer (on-demand)#authentication
    ```

4   Type the following command:

    ```
    Enforcer (authentication)# radius add name alias name server
    RADIUS sever address secret shared secretauth_method auth method
    ```

    where:

    - *alias_name* represents the name displayed for the RADIUS authentication method listed in **Auth Server** in the logon dialog box.

    - *RADIUS server address* represents the RADIUS server and port. Port is an optional number between 1 and 65535. If you do not specify a port number the Enforcer uses a default of port 1812.

    - *shared secret* is the shared secret on the RADIUS server.

    - *auth method* is PAP, CHAP, MS-CHAP-V1, or MS-CHAP-V2.

5   Type the following command:

    ```
    Enforcer (authentication)# radius enable
    ```

6   ```
    Enforcer (authentication#enable
    ```

In addition to the RADIUS add name and RADIUS enable commands, you can run other RADIUS commands to manage the RADIUS server.

See "Setting up user authentication with a RADIUS server" on page 1058.

## Setting up the On-Demand client on Windows for authentication with the dot1x-tls protocol

The Gateway Enforcer appliance can connect to dot1.x-enabled ports with the tls protocol.

**To set up the On-Demand client on Windows for authentication with the dot1x-tls protocol**

1   On the Enforcer console, type: `Enforcer#on-demand`

2   Type the following command: `Enforcer (on-demand)# dot1x`

3   Type the following command: `Enforcer (dot1x)# protocol tls`

4   Type the following command: `Enforcer (tls)# show protocol`

    The protocol must be set to tls. For example, `Active Protocol: TLS`

5   Type the following command: `Enforcer (tls)# validate-svr enable`

6   Type the following command: `Enforcer (cert-svr)# exit`

**7**   Type the following command: `Enforcer (tls)# show tls`

Make sure that the tls server certificate is enabled. For example:

```
TLS Validate Server Certificate:        ENABLED
TLS Certificate Server:                 ENABLED
TLS Certificate Server:                 127.0.0.1
```

8   Type the following command: `Enforcer (dot1x)# certificate import tftp 10.34.68.69 password symantec username janedoe user-cert qa.pfx root-cert qa.ce`

where:

`10.34.68.69` is the tftp server from which the Enforcer appliance can import the certificate by tftp.

`symantec` is the password of the user certificate

`janedoe` is the user name with which you log on the client.

`qa.pfx` is the name of the user certificate.

`qa.cer` is the name of the root certificate

Setting up the On-Demand client on Windows for authentication with the dot1x-peap protocol

Gateway Enforcer appliance can establish a connection with the peap protocol.

To set up the On-Demand client on Windows for authentication with the peap protocol

1   On the Enforcer console, type: `Enforcer#on-demand`

2   Type the following command: `Enforcer (on-demand)# dot1x`

3   Type the following command: `Enforcer (dot1x)# protocol peap`

4   Type the following command: `Enforcer (peap)# show protocol`

Make sure that the peap server certificate is enabled; for example:

```
PEAP Validate Server Certificate:       ENABLED
PEAP Certificate Server:                DISABLED
PEAP Certificate Server:                127.0.0.1
PEAP Fast Reconnected:                  DISABLED
```

5   If server validation is required, type:

```
Enforcer (peap) cert-svr host snac
```

where `snac` is the computer that is the CA server for the peap certificate name. Then type:

```
Enforcer (peap) exit
Enforcer (dot1x certificate import tftp 10.34.68.69 root-cert qa.cer
```

6   If no server validation is required, type:

```
Enforcer (peap) validate_svr disable
```

on-demand authentication commands

Set up user authentication for Symantec Network Access Control On-Demand clients from the Gateway Enforcer appliance console.

If you want to authenticate Symantec Network Access Control On-Demand clients on the Windows and Macintosh platforms, you can use any of the following:

- The local database that is resident on a Gateway Enforcer appliance.
  You can choose to use the local on-board database to add user names and passwords for individual users.

- Active Directory server configured to work with the Gateway Enforcer appliance.
  You must be able to connect to a Microsoft Windows Server 2003 Active Directory configured to work with a Gateway appliance.

- RADIUS Server
  You must be able to connect to one or more RADIUS servers.

Table 58-1 provides information about the on-demand authentication command.

Table 58-1   On-demand authentication arguments

Command	Description
ad	Enables authentication through the use of an Active Directory server instead of the on-board local database on a Gateway Enforcer appliance.

Table 58-1   On-demand authentication arguments *(continued)*

Command	Description
disable	Disables authentication of the Symantec Network Access Control On-Demand clients on the Gateway Enforcer. End users can trigger the automatic downloading of the Symantec Network Access Control On-Demand clients on a client computer without authentication. See "on-demand authentication disable" on page 1064.
default	Sets the authentication methods (Active Directory, on-board local database, or RADIUS server) guest users can select when they log on.
enable	Enables authentication of the Symantec Network Access Control On-Demand clients on the Gateway Enforcer appliances. Once enabled, an end-user must pass the authentication (input correct username and password) before downloading of the Symantec Network Access Control On-Demand clients. See "on-demand authentication enable" on page 1064.
local-db	Enables authentication through the use of the on-board local database on the Gateway Enforcer appliance.
radius	Enables authentication through a RADIUS server.
show	Lists the status information about the different options and arguments of the authentication command.
upload	Uploads authentication-related files to a server.

On-demand authentication default command

The on-demand authentication default command provides users with one or more authentication methods for logging on as guests. Configure Active Directory, local database, or one or more RADIUS server methods by using the on-demand default command. When more than one method has been configured, users select a method from the **Auth Server** drop-down list in the On-Demand client download **Welcome** screen.

The on-demand authentication default command uses the following syntax:

```
on-demand authentication default ad | radius | local-db index
```

Where:

ad, radius, and local-db represent the authentication method and index represents the index of the RADIUS server.

The following example describes how to specify the Active Directory and RADIUS server methods:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# default ad | radius radiusAuthServerIndex
```

on-demand authentication ad commands

If an enterprise network supports a Microsoft Windows Server 2003 Active Directory, you can authenticate users with an Active Directory server. Otherwise you must set up the on-board database or a RADIUS server to authenticate users.

on-demand authentication ad disable

The on-demand authentication ad disable command uses the following syntax to disable the authentication of clients with a Microsoft Windows Server 2003 Active Directory:

You must be logged on to the console of a Gateway Enforcer appliance as a superuser before you can execute this command.

The following example describes how to disable the authentication for an On-Demand client with a Microsoft Windows Server 2003 Active Directory:

```
on-demand authentication ad disable
```

on-demand authentication ad domain

The on-demand authentication ad domain command uses the following syntax to specify the domain ID or the domain ID address of a Microsoft Windows Server 2003 Active Directory:

```
on-demand authentication ad domain
Active Directory Domain domain name |
  name alias name
```

where:

Active Directory Domain domain name	Represents the domain name of a Microsoft Windows Server 2003 Active Directory.
alias name	Represents the name that is displayed for the Active Directory authentication method listed in **Auth Server** in the **Log on** dialog box.

The following example describes how to specify the domain ID of a Microsoft Windows Server 2003 Active Directory:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# ad domain symantec.com name symantec
```

where:

symantec.com represents the alias name displayed for Auth Server in the **Log on** dialog box.

on-demand authentication ad enable

The on-demand authentication ad enable command uses the following syntax for enabling the authentication of end users with a Microsoft Windows Server 2003 Active Directory:

```
on-demand authentication ad enable
```

The following example describes how to enable authentication for an On-Demand client with a Microsoft Windows Server 2003 Active Directory:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# ad enable
```

on-demand authentication enable

You can start the authentication process—the auth-daemon—on the console of a Gateway appliance for a Symantec Network Access Control On-Demand client.

The on-demand authentication enable command uses the following syntax:

```
on-demand authentication enable
```

You must be logged on a Gateway Enforcer appliance console as a superuser before you can execute this command.

The following example describes how to enable authentication for a Symantec Network Access Control On-Demand client on the console of a Gateway Enforcer appliance:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication enable
```

on-demand authentication disable

You can stop the authentication process—the auth-daemon—on the console of a Gateway appliance for a Symantec Network Access Control On-Demand client.

The on-demand authentication disable command uses the following syntax:

```
on-demand authentication disable
```

You must be logged on a Gateway Enforcer appliance console as a superuser before you can execute this command.

The following example describes how to disable authentication for a Symantec Network Access Control On-Demand client on the console of a Gateway Enforcer appliance:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication disable
```

on-demand authentication RADIUS server commands

To authenticate guest users with RADIUS servers, you must add a RADIUS server configuration on a Gateway Enforcer appliance. Once you add RADIUS servers, you can customize RADIUS attributes, or delete them.

See "Setting up user authentication with a RADIUS server" on page 1058.

You must be logged on the console of a Gateway Enforcer appliance as a superuser before you can execute this command.

on-demand authentication radius server add

The on-demand radius authentication add command syntax adds a RADIUS server configuration to a Gateway Enforcer appliance. This command uses the following syntax:

```
on-demand authentication radius add name alias_name server
RADIUS server address secret shared secret
auth method
```

where:

alias_name	The name that is displayed for the RADIUS authentication method listed in **Auth Server** in the logon dialog box
RADIUS server address	The RADIUS server address and port in the format of IP:*port* or host:*port*. You can accept the default port of 1812 or specify a port number between 1 and 65535.
	The RADIUS server alias name.
shared secret	The shared secret on the RADIUS server.

auth_method	One of the following authentication methods:

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication)
- MS-CHAP-1 (Microsoft CHAP, version 1)
- MS-CHAP-V2 (Microsoft CHAP, version 2)

The following examples describe how to add a RADIUS server:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# radius add name guests server
   IP:1812 shared secret8d#>9fq4bV)H7%a3-zE13sW CHAP
```

on-demand authentication local-db commands

Your enterprise can choose to authenticate users with the on-board database that you can set up on a Gateway Enforcer appliance Enforcer appliance.

on-demand authentication local-db add

If you choose to authenticate users with the on-board database, you must add user accounts for each client on a Gateway Enforcer appliance.

See "Setting up user authentication with a local database" on page 1057.

You must be logged on the console of a Gateway Enforcer appliance as a superuser before you can execute this command.

The on-demand local-db authentication add command uses the following syntax to add a user account to the on-board database that you set up on a Gateway Enforcer appliance.

```
on-demand authentication local-db add user username
```

where:

username represent a user account that you can add to the on-board database.

The following describes how to add to the local-db:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# local-db add user jim
```

on-demand authentication local-db enable

The on-demand local-db authentication enable command uses the following syntax to enable the on-board database that you can set up on a Gateway Enforcer appliance:

```
on-demand authentication local-db enable
```

The following example describes how to enable the local-db:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# local-db enable
```

on-demand authentication local-db disable

The on-demand local-db authentication disable command uses the following syntax to disable the on-board database that you set up on a Gateway Enforcer appliance:

```
on-demand authentication local-db disable
```

The following example describes how to disable the local-db:

```
Enforcer# on-demand
Enforcer (on-demand)# authentication
Enforcer (authentication)# local-db disable
```

on-demand authentication local-db username commands

The on-demand local-db authentication username commands let you add, delete, and edit user names:

```
local-db add username string password string
local-db delete username string
local-db edit username string password string
local-db enable |disable | clear
```

where:

add	Create a new user account to the local database
clear	Clean up all user accounts from the local database
delete	Remove an existing user from the local database
disable	Disable the local database authentication
edit	Modify an existing user account

enable	Enable local database authentication

The following example describes how to configure local database authentication for a Symantec Network Access Control On-Demand client on the console of a Gateway Enforcer appliance:

```
Enforcer# on-demand
Enforcer(on-demand)#authentication
Enforcer(authentication)# local-db disable
Local database authentication is disabled.

Enforcer(authentication)# local-db enable
Local database authentication is enabled.

Enforcer(authentication)# local add username test password test

Enforcer(authentication)# local-db delete username test
Your action will delete the user account "test" permanently.
  Please confirm. [Y/N]y

Enforcer(authentication)# local-db edit username test password b

Enforcer(authentication)# local-db clear
Notice that your action will remove ALL user account permanently!
  Please confirm. [Y/N]y
```

Editing the banner on the Welcome page

You can edit the default banner text on the **Welcome** page of the Symantec Network Access Control On-Demand client.

To edit the banner on the Welcome page

1   Log on to the Gateway Enforcer appliance console as a superuser.

    See "Logging on to an Enforcer appliance" on page 804.

2   Type the following command on the console of a Gateway Enforcer appliance:

    Enforcer# on-demand

3 Type the following command:

```
Enforcer(on-demand)# banner
```

Press **Enter**.

4 In the pop-up window, type the message that you want users to view on the **Welcome** page of the Symantec Network Access Control On-Demand client.

You can type up to 1024 characters.

Troubleshooting the Enforcer appliance

This chapter includes the following topics:

- Troubleshooting communication problems between an Enforcer appliance and the Symantec Endpoint Protection Manager

- Troubleshooting an Enforcer appliance

- Frequently asked questions for the Enforcer appliances

- Troubleshooting the connection between the Enforcer and the On-Demand Clients

Troubleshooting communication problems between an Enforcer appliance and the Symantec Endpoint Protection Manager

If the Enforcers and the management server do not communicate, look at the following possible reasons and solutions.

Table 59-1   Troubleshooting communication problems between Enforcers and the management server

Issue	Solution
Enforcer cannot register with the Symantec Endpoint Protection Manager	■ Check the management server configuration on Enforcer using the command `configure show spm`. Make sure that you have configured the management server IP address, port number, and pre-shared secret correctly. The default port number is 8014. ■ If the Enforcer type was re-configured or changed, delete the Enforcer group on the management server or move the Enforcer to a different group. For example, the Enforcer type might have changed from a Gateway Enforcer to a LAN Enforcer. ■ The management server list for the Enforcer might have a management server that the Enforcer cannot reach or has multiple interfaces of a management server. You might need to add a management server list with only one management server that can connect to the Enforcer. The management server must have one IP address.
Delay in connecting to the network through an Enforcer or the Gateway Enforcer appliance blocks clients	If you use a fail-open Enforcer, check the switch configuration. Make sure that PortFast is enabled on both ports to which the Enforcer connects.
Client disconnected events in the LAN Enforcer appliance's Client Log	If the clients frequently suspend and do not respond to re-authentication requests (802.1x EAP) from the switch, you may need to decrease the switch-re-authentication timeout.
LAN Enforcer appliance does not switch clients to the correct VLAN	■ Check that the selected switch model in the configuration matches the switch in use. ■ Check that the VLAN names exactly match what has been configured on the switch. ■ Check that the action table's VLAN assignments are correct for the switch in the management server console.

See "Frequently asked questions for the Enforcer appliances" on page 1073.

See "Troubleshooting an Enforcer appliance" on page 1073.

Troubleshooting an Enforcer appliance

Table 59-2 displays the possible problems and solutions you might have with an Enforcer appliance.

Table 59-2   Troubleshooting problems and solutions for an Enforcer appliance

Symptom	Solution
Enforcer root password is shown as invalid when set using the command-line interface	Limit passwords to 128-characters. Use another password of shorter length. See "About the Enforcer appliance CLI command hierarchy" on page 855.
Changing memory on the R200 causes hardware errors	The errors are due to hard coding of the IRQs. Remove the additional memory or reinstall the Enforcer after the hardware change. Our tests have shown that additional memory does not make an appreciable difference. See "Installing an Enforcer appliance" on page 800.
Some settings (Debug Level, Capture) return to default when the Enforcer is upgraded	A return to defaults can appear on upgrade, but does not appear thereafter. See "Upgrading the Enforcer appliance image" on page 809.
Problems appear when you are running SNMP with the Enforcer and HP OpenView	Resolve this problem by configuring HP OpenView: ■ Load the Symantec MIB file by selecting **Option > Load/unload MIB** ■ Using **Option > Event Configuration**, choose **OnDemandTraps (.1.3.6.1.4.1.393.588)**, and modify each trap as required. For example on **Event Message**, choose **Log and display in category**. Then select a category from the drop-down list. Set the **Event Log Message** as **$1**.

See "Troubleshooting communication problems between an Enforcer appliance and the Symantec Endpoint Protection Manager" on page 1071.

Frequently asked questions for the Enforcer appliances

The following issues provide answers about enforcement issues on the Gateway Enforcer appliance, or LAN Enforcer appliance:

- See "Which virus protection and antivirus software is managed by Host Integrity?" on page 1074.
- See "Can Host Integrity policies be set at the group level or the global level?" on page 1074.
- See "Can you create a custom Host Integrity message?" on page 1074.
- See "What happens if Enforcer appliances cannot communicate with Symantec Endpoint Protection Manager?" on page 1075.
- See "Is a RADIUS server required when a LAN Enforcer appliance runs in transparent mode?" on page 1076.
- See "How does enforcement manage computers without clients?" on page 1077.

Which virus protection and antivirus software is managed by Host Integrity?

Host Integrity enables you to add custom requirements to detect and manage virus protection software. In a custom requirement, you can specify virus protection applications and signature file information to check as part of your IF-THEN condition statement. The products that are supported appear in a drop-down list in the custom requirement dialog box.

See "About antivirus conditions" on page 831.

See "What you can do with Host Integrity policies" on page 812.

Can Host Integrity policies be set at the group level or the global level?

You can assign Host Integrity policies by group and by location on the console of the Symantec Endpoint Protection Manager.

See "Creating and testing a Host Integrity policy" on page 812.

Can you create a custom Host Integrity message?

Symantec Network Access Control can create custom Host Integrity messages for each Host Integrity rule. You can customize the message, including the icon and the title. You can perform this customization through a custom Host Integrity rule.

See "Displaying a message dialog box" on page 843.

What happens if Enforcer appliances cannot communicate with Symantec Endpoint Protection Manager?

If you plan to use Enforcers with Symantec Endpoint Protection, we recommend that you have redundant management servers. If the Symantec Endpoint Protection Manager is unavailable, the Enforcer blocks the traffic from the clients.

Redundant management servers are preferable. The Enforcer sends a UDP packet on port 1812 by using the RADIUS protocol to the Symantec Endpoint Protection Manager to verify the GUID from the clients. If a firewall blocks this port or if a Symantec Endpoint Protection Manager is unavailable, then the clients are blocked.

An option on the Enforcer allows client access to the network when the Symantec Endpoint Protection Manager is unavailable. If this option is enabled and the Symantec Endpoint Protection Manager is unavailable, the GUID check and the profile checks are not performed. Only the Host Integrity check can be performed on the client when the Symantec Endpoint Protection Manager is unavailable.

You can use the advanced local-auth command to enable or disable the Enforcer's authentication of a client.

advanced local-auth

The advanced local-auth command enables or disables the Enforcer's authentication of the client. Use this command for troubleshooting.

Client authentication is disabled by default.

The advanced local-auth command uses the following syntax:

```
advanced local-auth {disable | enable}
```

where:

Disable	Verifies the Agent with the management server. This blocks the Agent if it is unable to connect to a management server.
	The default setting for client authentication is Disable.
Enable	Disables Agent verification and performs Host Integrity validation only.

By default, the Gateway Enforcer appliance verifies the globally unique identifier (GUID) of the client with the Symantec Endpoint Protection Manager. If the Gateway Enforcer is unable to connect with a Symantec Endpoint Protection Manager to verify the GUID, it blocks the client. Although it is not recommended

as a troubleshooting step, you can stop the Gateway Enforcer appliance from verifying the GUID.

By default, the Gateway Enforcer appliance verifies the GUID. Instead, the Gateway Enforcer appliance only performs a Host Integrity validation check. Be sure to re-enable this setting if you want the Gateway Enforcer appliance to verify the GUID.

See "Communication between an Enforcer appliance and a Symantec Endpoint Protection Manager" on page 786.

Is a RADIUS server required when a LAN Enforcer appliance runs in transparent mode?

RADIUS server requirements depend on how the switch is configured and what you use the switch to authenticate.

The following are some items to watch out for:

- Switches that use RADIUS servers for more than the authentication of 802.1x users.
  For example, when you log on to the switch, you must type a user name and password. The RADIUS server typically performs authentication for this logon. When the LAN Enforcer appliance is installed, this authentication is sent to the LAN Enforcer appliance. If the authentication is sent to the LAN Enforcer appliance, you must configure the RADIUS server IP address in the LAN Enforcer appliance. You must configure the LAN Enforcer appliance to forward all non-EAP requests directly to the RADIUS server.

- Installation of a 802.1x supplicant on a client system. If an 802.1x supplicant exists on a client system, the LAN Enforcer appliance tries to authenticate with the RADIUS server. 802.1x authentication is enabled by default on Windows XP. If you enable your client to work in transparent mode, it does not automatically disable the built-in 802.1x supplicant. You must make sure that no 802.1x supplicant runs on any of your client computers.

- Configuration of the Enforcer to ignore the RADIUS request from any client computer that includes a third-party 802.1x supplicant. You can set up this configuration by using an IP address of 0.0.0.0 for the RADIUS server. You can use this setup if you want to run a LAN Enforcer in transparent mode. Some clients can have an 802.1x supplicant. In this case, you can specify that the LAN Enforcer appliance does not send any traffic to a RADIUS server.

See "Using RADIUS server group settings" on page 926.

How does enforcement manage computers without clients?

Symantec Network Access Control can enforce security policies only for the systems that have Symantec clients installed. The security stance of other vendors cannot be enforced. Any enforcement by other vendors can disrupt the network.

The following enforcement methods are available:

Self enforcement	Self enforcement by the client firewall has no effect on the systems without clients in the network.
	See "How self enforcement works" on page 783.
Gateway enforcement	In the networks that use gateway enforcement, the systems without clients cannot pass through the gateway. Where you place the Gateway Enforcer in the network is critical; it can block access to critical network resources to which other systems require access.
	You can make exceptions for trusted IP addresses so that they can pass through the gateway inbound or outbound without a client. Similarly, the gateway can also exempt non-Microsoft operating systems from enforcement. One network design can be to place non-critical servers on the same side of the gateway. This configuration simplifies the network design without seriously compromising security.
	See "How the Gateway Enforcer appliance works" on page 787.
DHCP enforcement	DHCP enforcement restricts the computers that are out of compliance or the systems without clients. It restricts these systems to a separate address space or provides them with a subset of routes on the network. This restriction reduces the network services for these devices. Similar to gateway enforcement, you can make exceptions for trusted MAC addresses and non-Microsoft operating systems.
	See "How an Integrated Enforcer for Microsoft DHCP Servers works" on page 790.

LAN enforcement	LAN enforcement uses the 802.1x protocol to authenticate between the switch and the client systems that connect to the network. To use this method of enforcement, the switch software must support the 802.1x protocol and its configuration must be correct. 802.1x supplicant software is also required if the administrator wants to verify user identity as well has host NAC status. The switch configuration must handle the exceptions for systems without clients, rather than any Symantec configuration.
	You have several ways to set up this switch configuration. Methods vary depending on the type of switch and software version it runs. A typical method implements the concept of a guest VLAN. Systems without clients are assigned to a network that has a lower level of network connectivity. Another method involves basing the exceptions on MAC addresses.
	You can disable 802.1x on selected ports. However, to disable by selected ports allows anyone to connect by using the port, so it is not recommended. Many vendors have special provisions for the VoIP phones that can automatically move these devices to special voice VLANs.
	See "How the LAN Enforcer appliance works" on page 788.
Universal enforcement API	When you use the Universal Enforcement API, the third-party vendor's implementation of the API handles the exceptions.
Enforcement by using Cisco NAC	When you use the Symantec solution to interface with Cisco NAC, the Cisco NAC architecture handles any exclusions.

About debug information transfer over the network

When problems occur on the Enforcer appliance, a debug log is created on the Enforcer (kernel.log). If you need to transfer debug information over the network, use one of the following debug commands to transfer the debug logs:

debug upload	To transfer one file to a tftp server

File transfer over the network requires a serial connection between a computer and the Enforcer appliance.

The following example represents a file-transfer output that the HyperTerminal performs:

```
<date>          <Time>      <File Name>
2008-08-01  16:32:26    user.log
2008-08-01  16:32:24    kernel.log
2008-08-01  14:30:03    ServerSylink[04-05-2010-14-30-03].xml
2008-08-01  14:29:59    ServerProfile[04-05-2010-14-29-59].xml
Enforcer(debug)# upload tftp 10.1.1.1 filename kernel.log
```

See

Troubleshooting the connection between the Enforcer and the On-Demand Clients

There are several areas and known issues that you may check to troubleshoot your connection between the Enforcer and On-Demand clients.

Table 59-3 Connection troubleshooting

Symptom	Solution
Firewall is blocking the client from working when the user downloads the agent through PPTP VPN, CheckPoint VPN, or Juniper VPN.	Several possible solutions: ■ Change firewall settings to unblock UDP port 39999. ■ Add a static route to the Enforcer's route table. For example: `route add IP netmask NM device eth0` where IP and NM are the IP address and netmask of the client's IP address pool. This pool is configured on the VPN by the administrator.
Download times are sometimes long.	The client sometimes sends traffic to VeriSign, making the download speed somewhat long. A workaround is let the admin add the VeriSign to the trusted IP list.
Host Integrity check is sometimes long the first time.	A long Host Integrity check is an issue with DNS resolution, and should not appear after the first Host Integrity check.
Firewall on the client is blocking the On-Demand client from working when the user does not have Admin rights	Users should change firewall settings to unblock UDP port 39999. Alternatively, set the firewall with the following: `cclientctl.exe`

Table 59-3 Connection troubleshooting *(continued)*

Symptom	Solution
Upgrading the Enforcer does not initially contain the manual installation package.	This problem is due to the size of the packages taken together. The workaround is to upgrade the Enforcer and import the Client Manual Install Package on Symantec Endpoint Protection Manager first, and then enable On-Demand functionality on the Enforcer. That adds the manual installation files.
The redirect URL on the Enforcer will overwrite a previous redirect URL on Symantec Endpoint Protection Manager.	The redirect URL overwrite problem only happens when the On-Demand feature is enabled on the Enforcer. This is expected behavior.
Vista clients sometimes do not receive an IP address from the DHCP server.	This problem is a timing issue. Change the DHCP timeout setting to 12 seconds or more.
A normal user can not install the agent if JRE is not installed.	The workaround is to ensure that JRE is installed. Otherwise only Admin users can install JRE.
Wireless service is disconnected when the On-Demand client is installed and quits and 802.1x authentication is used.	The user should restart the wireless connection.
Systems that are running Norton 360 v. 2.x have a problem receiving the client.	To solve this problem, follow the manual download link to download and install and install the client.
With Firefox, you cannot download the client and NP Plugin with only user rights.	Installation of the NP plugin requires Admin rights.
Manual installation sometimes fails.	To solve this problem, you may need to install Microsoft patch KB893803. This patch is included with the manual install, and should be installed before the client installation. Admin privileges are required.
802.1x authentication fails	The agent needs to install a driver to work. If the user needs 802.1x authentication on Windows Vista, the user needs to open the browser with the "Run as Administrator" method or turn off UAC to make sure that the agent works with Administrator privileges.
"Old version of ActiveX detected" message appears	You should delete the existing ActiveX by clicking **Tools -> Manage Add-ons -> Enable or Disable Add-ons -> Downloaded ActiveX Controls**, and deleting **HodaAgt class**.

Table 59-3   Connection troubleshooting *(continued)*

Symptom	Solution
Browser notifies the user , "can not display webpage," and the client cannot download successfully.	The client may already be running. As a security feature, you cannot download a new client inside of a running client session.
Firefox browser sometimes cannot download the client.	This problem happens when Firefox runs first. The first few Firefox restarts are required for it to finish its configuration. After that the On-Demand client should download.
Computers running Mac OS 10.4 sometimes do not authenticate properly due to a changing hostname.	This appears to be a problem with this version of the Mac OS. Version 10.5 and later does not have the problem. The workaround for version 10.4 is to set the hostname in `/etc/hostconfig/`.
Custom Host Integrity checks that rely upon the system variable %temp% do not work.	This is because of the transitory nature of %temp%. The workaround is to point to different locations.
Custom Host Integrity rules that point to Windows registry values do not work properly.	This is because of the transient nature of user sessions.
Installation of Panda Titanium 2007 or Panda Internet Security 2007 or 2008 software causes a message to appear, "Please wait while Windows configures Symantec Network Access Control."	Panda deletes a crucial Symantec Network Access Control file. It is automatically reinstalled, and you may safely take no action.
Mac client transparent mode dot1x authentication sometimes fails	The Mac on-demand client is not compatible with PEAP authentication. If your Mac is configured for PEAP authentication, you must disable it in your network connection properties on the Mac. Transparent mode dot1x authentication then works fine.
On Windows Vista, the on-demand client fails to authenticate properly when using PEAP and a custom VSA	This problem is specific to using a custom VSA and PEAP authentication on Windows Vista. The workaround is to use a different form of authentication.

Differences between Mac and Windows features

This appendix includes the following topics:

- Client protection features by platform

- Management features by platform

- Virus and Spyware Protection policy settings available for Windows and Mac

- LiveUpdate policy settings available for Windows and Mac

Client protection features by platform

Table A-1 explains the differences in the protection features that are available on the different client computer platforms.

Table A-1   Symantec Endpoint Protection client protection

Client feature	Windows XP (SP2), Windows Vista, Windows 7, Windows 8, 32-bit	Windows XP (SP2), Windows Vista, Windows 7, Windows 8, 64-bit	Windows Server 2003, Windows Server 2008, 32-bit	Windows Server 2003, Windows Server 2008, Windows Server 2012, 64-bit	Mac	Linux
Scheduled scans	Yes	Yes	Yes	Yes	Yes	Yes
On-demand scans	Yes	Yes	Yes	Yes	Yes	Yes
Auto-Protect for the file system	Yes	Yes	Yes	Yes	Yes	Yes

	Table A-1		Symantec Endpoint Protection client protection *(continued)*			

Client feature	Windows XP (SP2), Windows Vista, Windows 7, Windows 8, 32-bit	Windows XP (SP2), Windows Vista, Windows 7, Windows 8, 64-bit	Windows Server 2003, Windows Server 2008, 32-bit	Windows Server 2003, Windows Server 2008, Windows Server 2012, 64-bit	Mac	Linux
Internet Email Auto-Protect	Yes	Yes	No	No	No	No
Microsoft Outlook Auto-Protect	Yes	Yes	Yes	Yes	No	No
Lotus Notes Auto-Protect	Yes	Yes	Yes	Yes	No	No
SONAR	Yes	Yes	Yes	Yes	No	No
Firewall	Yes	Yes	Yes	Yes	No	No
Intrusion Prevention	Yes	Yes	Yes	Yes	No	No
Application and Device Control	Yes	Yes	Yes	Yes	No	No
Host Integrity	Yes	Yes	Yes	Yes	No	No
Tamper Protection	Yes	Yes, with limitations	Yes	Yes, with limitations	No	No

Management features by platform

Table A-2 explains the management features that are available for the Windows and Mac client platforms.

Table A-2   Comparison between Symantec Endpoint Protection Manager
                   features for Windows and Mac

Feature	Windows	Mac
Deploy client remotely from Symantec Endpoint Protection Manager	Yes	No
Manage client from Symantec Endpoint Protection Manager	Yes	Yes
Update virus definitions and product from management server	Yes	No
Run commands from management server	■ Scan ■ Update Content ■ Update Content and Scan ■ Restart Client Computers ■ Enable Auto-Protect ■ Restart Client Computers ■ Enable Auto-Protect ■ Enable Network Threat Protection ■ Disable Network Threat Protection	■ Scan ■ Update Content ■ Update Content and Scan ■ Restart Client Computers ■ Enable Auto-Protect ■ Restart Client Computers ■ Enable Auto-Protect
Provide updates by using Group Update Providers	Yes	No
Run Intelligent Updater	Yes	Yes
Package updates for third-party tools in management server	Yes	No*
Set randomized scans	Yes	No
Set randomized updates	Yes	Yes

*You can run Intelligent Updater to get Mac content updates. You can then push
the updates to Mac clients by using a third-party tool such as Apple Remote
Desktop.

See "Using Intelligent Updater files to update client virus and security risk
definitions" on page 593.

See "Virus and Spyware Protection policy settings available for Windows and
Mac" on page 1086.

See "LiveUpdate policy settings available for Windows and Mac" on page 1087.

Virus and Spyware Protection policy settings available for Windows and Mac

Table A-3 displays the differences in the policy settings that are available for Windows clients and Mac clients.

Table A-3   Virus and Spyware Protection policy settings (Windows and Mac only)

Policy setting	Windows	Mac
Define actions for scans	You can specify first and second actions when different types of virus or risk are found. You can specify the following actions: ■ Clean ■ Quarantine ■ Delete ■ Leave alone	You can specify either of the following actions: ■ Automatically repair infected files ■ Quarantine files that cannot be repaired
Specify remediation if a virus or a risk is found	You can specify the following remediation actions: ■ Back up files before repair ■ Terminate processes ■ Stop services	Remediation is automatically associated with actions.
Set scan type	Active, Full, Custom	Custom only
Retry scheduled scans	Yes	No
Set scans to check additional locations (scan enhancement)	Yes	No
Configure storage migration scans	Yes	No
Configure scan exceptions	Yes	Yes
Scan on mount	No	No

LiveUpdate policy settings available for Windows and Mac

Table A-4 displays the LiveUpdate Settings policy options that the Windows client and the Mac client support.

Table A-4   LiveUpdate policy settings (Windows and Mac only)

Policy setting	Windows	Mac
Use the default management server	Yes	No
Use a LiveUpdate server (internal or external)	Yes	Yes
Use a Group Update Provider	Yes	No
Enable third-party content management	Yes	No You can, however, run Intelligent Updater to get Mac content updates. You can then push the updates to Mac clients by using a third-party tool such as Apple Remote Desktop.
LiveUpdate Proxy Configuration	Yes	Yes, but it is not configured in the LiveUpdate policy. To configure this setting, click **Clients** > **Policies**, and then click **External Communications Settings**.
LiveUpdate Scheduling	Yes	Yes, for **Frequency** and **Download Randomization** options; no for all other scheduling options
User Settings	Yes	No
Product Update Settings	Yes	Yes
HTTP Headers	Yes	No

See "Virus and Spyware Protection policy settings available for Windows and Mac" on page 1086.

See "Client protection features by platform" on page 1083.

Customizing and deploying the client installation by using third-party tools

This appendix includes the following topics:

- Installing client software using third-party tools

- About client installation features and properties

- Symantec Endpoint Protection client installation properties

- Symantec Endpoint Protection client features

- Windows Installer parameters

- Windows Security Center properties

- Command-line examples for installing the client

- About installing and deploying client software with the Symantec Management Agent

- Installing clients with Microsoft SMS 2003

- Installing clients with Active Directory Group Policy Object

- Uninstalling client software with Active Directory Group Policy Object

Installing client software using third-party tools

You can install the client using third-party tools instead of the tools that are installed with the management server. If you have a large network, you are more likely to benefit by using these options to install Symantec client software.

You can install the client by using a variety of third-party products. These products include Microsoft Active Directory, Tivoli, Microsoft Systems Management Server (SMS), and Novell ZENworks. Symantec Endpoint Protection supports Novell ZENworks, Microsoft Active Directory, and Microsoft SMS.

Table B-1 displays the third-party software and tools that you can use to install the client

Table B-1   Third-party tools to install the client

Tool	Description
Windows .msi command-line tools	The Symantec client software installation packages are Windows Installer (.msi) files that you can configure by using the standard Windows Installer options. You can use the environment management tools that support .msi deployment, such as Active Directory or Tivoli, to install clients on your network. You can configure how the Windows Security Center interacts with the unmanaged client.
	See "About client installation features and properties" on page 1091.
	See "About configuring MSI command strings" on page 1092.
	See "About configuring Setaid.ini" on page 1092.
	See "Symantec Endpoint Protection client features" on page 1094.
	See "Symantec Endpoint Protection client installation properties" on page 1093.
	See "Windows Installer parameters" on page 1096.
	See "Command-line examples for installing the client" on page 1099.
	See "Windows Security Center properties" on page 1098.

Table B-1	Third-party tools to install the client *(continued)*
Tool	**Description**
Altiris Agent or Symantec Management Agent	You can install the client using the Symantec Integration Component. See "About installing and deploying client software with the Symantec Management Agent" on page 1099.
Microsoft SMS 2003	You can install the client by using Microsoft Systems Management Server. See "Installing clients with Microsoft SMS 2003" on page 1100.
Windows Active Directory	You can use the Windows 2000/2003/2008 Active Directory Group Policy Object if the client computers and are members of a Windows 2000/2003/2008 Active Directory domain. The client computers must also use a supported Windows operating system. See "Installing clients with Active Directory Group Policy Object" on page 1101. See "Uninstalling client software with Active Directory Group Policy Object" on page 1108.
Virtualization software	You can install the client in virtual environments. See "Supported virtual installations and virtualization products" on page 83.

See "Deploying clients by using Save Package" on page 137.

About client installation features and properties

Installation features and properties appear as strings in text files and command lines. Text files and command lines are processed during all client software installations. Installation features control which components get installed. Installation properties control which subcomponents are enabled or disabled after installation. Installation features and properties are available for Symantec Endpoint Protection client software only and are also available for the Windows operating system. Installation features and properties are not available for Symantec Network Access Control client software or for Symantec Endpoint Protection Manager installations.

Installation features and properties are specified in two ways: as lines in the Setaid.ini file and as values in Windows Installer (MSI) commands. MSI commands

can be specified in Windows Installer strings and in vpremote.dat for customized Push Deployment Wizard deployment. Windows Installer commands and Setaid.ini are always processed for all managed client software installations. If different values are specified, the values in Setaid.ini always take precedence.

About configuring MSI command strings

Symantec Endpoint Protection installation software uses Windows Installer (MSI) 3.1 or later packages for installation and deployment. If you use the command line to deploy a package, you can customize the installation. You can use the standard Windows Installer parameters and the Symantec-specific features and properties.

To use the Windows Installer, elevated privileges are required. If you try the installation without elevated privileges, the installation may fail without notice. For the most up-to-date list of Symantec installation commands and parameters, see the Symantec Support knowledge base article, MSI command line reference for Symantec Endpoint Protection.

Note: The Windows Installer advertise function is unsupported. Setaid.ini-specified features and properties take precedence over MSI-specified features and properties. Feature and property names in MSI commands are case sensitive.

See "About configuring Setaid.ini" on page 1092.

About configuring Setaid.ini

Setaid.ini appears in all installation packages and controls many of the aspects of the installation, such as which features are installed. Setaid.ini always takes precedence over any setting that may appear in an MSI command string that is used to start the installation. Setaid.ini appears in the same directory as setup.exe. If you export to a single .exe file, you cannot configure Setaid.ini. However, the file is automatically configured when you export Symantec Endpoint Protection client installation files from the console.

The following lines show some of the options that you can configure in Setaid.ini.

```
[CUSTOM_SMC_CONFIG]
InstallationLogDir=
DestinationDirectory=

[FEATURE_SELECTION]
Core=1

SAVMain=1
```

```
Download=1
OutlookSnapin=1
Pop3Smtp=0
NotesSnapin=0

PTPMain=1
 DCMain=1
 TruScan=1
```

Note: The features are indented to show hierarchy. The features are not indented inside the Setaid.ini file. Feature names in Setaid.ini are case sensitive.

Feature values that are set to 1 install the features. Feature values that are set to 0 do not install the features. You must specify and install the parent features to successfully install the client features.

See "Symantec Endpoint Protection client features" on page 1094.

Be aware of the following additional setaid.ini settings that map to MSI properties for Symantec Endpoint Protection client installation:

- DestinationDirectory maps to PRODUCTINSTALLDIR

- KeepPreviousSetting maps to MIGRATESETTINGS

- AddProgramIntoStartMenu maps to ADDSTARTMENUICON

Symantec Endpoint Protection client installation properties

These installation properties are for use with MSI command line installations.

Table B-2   Symantec Endpoint Protection client installation properties

Property	Description
RUNLIVEUPDATE =*val*	Determines whether LiveUpdate is run as part of the installation, where *val* is one of the following values: ■ 1: Runs LiveUpdate during installation (default). ■ 0: Does not run LiveUpdate during installation. By default, all Symantec Endpoint Protection clients in a group receive the latest versions of all content and all product updates. If the clients are configured to get updates from a management server, the clients receive only the updates that the server downloads. If the LiveUpdate content policy allows all updates, but the management server does not download all updates, the clients receive only what the server downloads.
ENABLEAUTOPROTECT =*val*	Determines whether File System Auto-Protect is enabled after the installation is complete, where *val* is one of the following values: ■ 1: Enables Auto-Protect after installation (default). ■ 0: Disables Auto-Protect after installation.
SYMPROTECTDISABLED =*val*	Determines whether Tamper Protection is enabled as part of the installation, where *val* is one of the following values: ■ 1: Disables Tamper Protection after installation. ■ 0: Enables Tamper Protection after installation. (default)

Symantec Endpoint Protection client features

Table B-3 lists the Symantec Endpoint Protection features can be installed by specifying them in Setaid.ini files and in MSI commands. Most features have a parent-child relationship. If you want to install a child feature that has a parent feature, you must also install the parent feature.

For both setaid.ini and MSI, if you specify a child feature but do not specify its parent feature, the child feature is installed. However, the feature does not work because the parent feature is not installed. For example, if you specify to install the Firewall feature but do not specify to install NTPMain, the firewall is not installed.

Table B-3   Symantec Endpoint Protection client features

Feature	Description	Required parent features
Core	Installs the files that are used for communications between clients and the Symantec Endpoint Protection Manager. This feature is required.	none
SAVMain	Installs the virus, spyware, and basic download protection. Subfeatures install additional protection.	Core
Download	Installs the complete protection for downloaded files. Includes fully functional reputation scanning by Download Insight.	SAVMain
NotesSnapin	Installs the Lotus Notes Auto-Protect email feature.	SAVMain
OutlookSnapin	Installs the Microsoft Exchange Auto-Protect email feature.	SAVMain
Pop3Smtp	Installs the protection for POP3 and SMTP mail. Available only on 32-bit systems.	SAVMain
PTPMain	Installs the Proactive Threat Protection components.	Core
TruScan	Installs the SONAR scanning feature.	PTPMain
DCMain	Installs the Application Control and Device Control feature.	PTPMain
NTPMain	Installs the Network Threat Protection components.	Core
ITPMain	Installs the Network and Intrusion Prevention and Browser Intrusion Prevention feature.	NTPMain
Firewall	Installs the firewall feature.	NTPMain
LANG1033	Installs English resources.	Core

Windows Installer parameters

Symantec Endpoint Protection client installation packages use the standard Windows Installer parameters, as well as a set of extensions for command-line installation and deployment.

See the Windows Installer documentation for further information about the usage of standard Windows Installer parameters. You can also execute msiexec.exe from a command line to see the complete list of parameters.

Table B-4   Windows Installer parameters

Parameter	Description
Sep.msi (32-bit) Sep64.msi (64-bit)	The .msi installation file for the Symantec Endpoint Protection client. If any .msi file contains spaces, enclose the file name in quotations when used with /I and /x. Required
Msiexec	Windows Installer executable. Required
/I ".*msi file name*"	Install the specified .msi file. If the file name contains spaces, enclose the file name in quotations. If the .msi file is not in the same directory from which you execute Msiexec, specify the path name. If the path name contains spaces, enclose the path name in quotations. For example, msiexec.exe /I "C:*path to* Sep.msi" Required
/qn	Install silently. **Note:** When a silent deployment is used, the applications that plug into Symantec Endpoint Protection, such as Microsoft Outlook and Lotus Notes, must be restarted after installation.
/x ".*msi file name*"	Uninstall the specified components. Optional
/qb	Install with a basic user interface that shows the installation progress. Optional
/l*v *logfilename*	Create a verbose log file, where *logfilename* is the name of the log file you want to create. Optional

Table B-4   Windows Installer parameters *(continued)*

Parameter	Description
PRODUCTINSTALLDIR=*path*	Designate a custom path on the target computer where *path* is the specified target directory. If the path includes spaces, enclose the path in quotation marks. **Note:** The default directory is C:\Program Files\Symantec\Symantec Endpoint Protection Optional
REBOOT=*value*	Controls a computer restart after installation, where *value* is a valid argument. The valid arguments include the following: ■ Force: Requires that the computer is restarted. Required for uninstallation. ■ Suppress: Prevents most restarts. ■ ReallySuppress: Prevents all restarts as part of the installation process, even a silent installation. Optional **Note:** Use ReallySuppress to suppress a restart when you perform a silent uninstallation of Symantec Endpoint Protection client.
ADDLOCAL= *feature*	Select the custom features to be installed, where *feature* is a specified component or list of components. If this property is not used, all applicable features are installed by default, and Auto-Protect email clients are installed only for detected email programs. To add all appropriate features for the client installations, use the ALL command as in ADDLOCAL=ALL. See "Symantec Endpoint Protection client features" on page 1094. **Note:** When you specify a new feature to install, you must include the names of the features that are already installed that you want to keep. If you do not specify the features that you want to keep, Windows Installer removes them. By specifying existing features, you do not overwrite the installed features. To uninstall an existing feature, use the REMOVE command. Optional
REMOVE=*feature*	Uninstall the previously installed program or a specific feature from the installed program, where *feature* is one of the following: ■ *Feature*: Uninstalls the feature or list of features from the target computer. ■ ALL: Uninstalls the program and all of the installed features. All is the default if a feature is not specified. Optional

Windows Security Center properties

You can customize Windows Security Center (WSC) properties during Symantec Endpoint Protection client installation. These properties apply to unmanaged clients only. Symantec Endpoint Protection Manager controls these properties for the managed clients.

Note: These properties apply to Windows XP Service Pack 2 or Service Pack 3. They do not apply to clients that run Windows Vista, and do not apply to Windows Action Center in Windows 7 and Windows 8.

Table B-5 Windows Security Center properties

Property	Description
WSCCONTROL=*val*	Controls WSC where *val* is one of the following values: ■ 0: Do not control (default). ■ 1: Disable one time, the first time it is detected. ■ 2: Disable always. ■ 3: Restore if disabled.
WSCAVALERT=*val*	Configures the antivirus alerts for WSC where *val* is one of the following values: ■ 0: Enable. ■ 1: Disable (default). ■ 2: Do not control.
WSCFWALERT=*val*	Configures the firewall alerts for WSC where *val* is one of the following values: ■ 0: Enable. ■ 1: Disable (default). ■ 2: Do not control.
WSCAVUPTODATE=*val*	Configures the WSC out-of-date time for antivirus definitions where *val* is one of the following values: 1 - 90: Number of days (default is 30).
DISABLEDEFENDER=*val*	Determines whether to disable Windows Defender during installation, where *val* is one of the following values: ■ 1: Disables Windows Defender (default). ■ 0: Does not disable Windows Defender.

Command-line examples for installing the client

Table B-6   Command-line examples

Task	Command line
Silently install all of the Symantec Endpoint Protection client components with default settings to the directory C:\SFN. Suppress a computer restart, and create a verbose log file.	msiexec /I "SEP.msi" PRODUCTINSTALLDIR=C:\SFN REBOOT=ReallySuppress /qn /l*v c:\temp\msi.log
Silently install the Symantec Endpoint Protection client with Virus and Spyware Protection, and with Network Threat Protection. Create a verbose log file. The computer must be restarted to implement Network Threat Protection.	msiexec /I "SEP.msi" ADDLOCAL=Core,SAVMain,EMailTools,OutlookSnapin, Pop3Smtp,ITPMain,Firewall /qn /l*v c:\temp\msi.log

About installing and deploying client software with the Symantec Management Agent

You can install and deploy Symantec client software on Windows computers by using Altiris software, now called the Symantec Management Agent. Symantec Endpoint Protection provides a free Integration Component for Symantec Endpoint Protection that provides default installation capabilities, integrated client management, and high-level reporting.

The Symantec Management Agent enables information technology organizations to manage, secure, and service heterogeneous IT assets. It also supports software delivery, patch management, and many other management capabilities. Altiris software helps IT align services to drive business objectives, deliver audit-ready security, automate tasks, and reduce the cost and complexity of management.

For the Symantec Endpoint Protection Integration Component documentation and installation file, see the Tools/SEPIntegrationComponent directory on the product disc.

For information about the Altiris product family, go to the following URL:

http://www.symantec.com/configuration-management

Installing clients with Microsoft SMS 2003

You can use Microsoft Systems Management Server (SMS) to install Symantec client software. We assume that system administrators who use SMS have previously installed software with SMS. As a result, we assume that you do not need detailed information about installing Symantec client software with SMS.

Note: This topic also applies to Microsoft System Center Configuration Manager (SCCM).

Symantec client installation software requires that Windows Installer 3.1 or later is present on client computers before the installation. This software is automatically installed if it is not present on client computers, but only when you deploy with a single executable setup.exe. This software is not automatically installed if you deploy with the MSI file. Computers that run Windows Server 2003 with Service Pack 2, and Windows Vista include Windows Installer 3.1 or later. If necessary, first deploy WindowsInstaller-x86.exe that is contained on the Symantec Endpoint Protection and the Symantec Network Access Control product disc. Upgrading the Windows Installer version also requires a computer restart.

Note: This note applies to SMS version 2.0 and earlier: If you use SMS, turn off the **Show Status Icon On The Toolbar For All System Activity** feature on the clients in the **Advertised Programs Monitor**. In some situations, Setup.exe might need to update a shared file that is in use by the Advertised Programs Monitor. If the file is in use, the installation fails.

Symantec recommends that SMS/SCCM packages launch Setup.exe rather than the MSI directly. This method ensures that the MSI engine can update to the minimum recommended version and also enables installer logging. Use the custom package creation feature in SMS/SCCM to create custom packages instead of the package wizard feature.

Warning: You must include a Sylink.xml file in the client installation packages that you created by using the files on the product disc. You must include a Sylink.xml file that is created after you install and use Symantec Endpoint Protection Manager. The Sylink.xml file identifies the management server to which the clients report. If you do not include this file the client is installed as an unmanaged client. As a result, all clients are installed with default settings and do not communicate with a management server.

Table B-7 lists the tasks to create and distribute Symantec client software with SMS 2003.

Table B-7   Process for installing the client using Microsoft Systems Management Server

Step	Description
Step 1	Create a software installation package with Symantec Endpoint Protection Manager that contains the software and policies to install on your client computers. Additionally, this software installation package must contain a file named Sylink.xml, which identifies the server that manages the clients.
Step 2	Create a source directory and copy Symantec client installation files into that source directory. For example, you would create a source directory that contains the installation files for Symantec client software.
Step 3	Create a package, name the package, and identify the source directory as part of the package.
Step 4	Configure the Program dialog box for the package to specify the executable that starts the installation process, and possibly specify the MSI with parameters.
Step 5	Distribute the software to specific Collections with Advertising.

For more information on using SMS/SCCM, see the Microsoft documentation that is appropriate for your version.

Installing clients with Active Directory Group Policy Object

You can install the client by using a Windows 2000/2003/2008 Active Directory Group Policy Object. The procedures assume that you have installed this software and use Windows Active Directory for installing client software with Active Directory Group Policy Object.

The installation software requires that client computers contain and can run Windows Installer 3.1 or later. Computers already meet this requirement if they run Windows XP with Service Pack 2 and higher, Windows Server 2003 with Service Pack 1 and higher, and Windows Vista/7/8/Server 2008/Server 2012. If client computers do not meet this requirement, all other installation methods automatically install Windows Installer 3.1 by bootstrapping it from the installation files.

For security reasons, Windows Group Policy Object does not permit bootstrapping to the executable file WindowsInstaller*.exe from the installation files. Therefore, before you install Symantec client software, you must run this file on the computers without Windows Installer 3.1 or later. You can run this file with a computer startup script. If you use a GPO as an installation method, you must decide how to update the client computers with Windows Installer 3.1 or later.

The Symantec client installation uses standard Windows Installer .msi files. As a result, you can customize the client installation with .msi properties.

See "About configuring MSI command strings" on page 1092.

You should confirm that your DNS server is set up correctly before deployment. The correct setup is required because Active Directory relies on your DNS server for computer communication. To test the setup, you can ping the Windows Active Directory computer, and then ping in the opposite direction. Use the fully qualified domain name. The use of the computer name alone does not call for a new DNS lookup. Use the following format:

```
ping computername.fullyqualifieddomainname.com
```

Table B-8   Steps for installing the client software by using Active Directory Group Policy Object

Step	Action
Step 1	Create the administrative install image. See "Creating the administrative installation image" on page 1103.
Step 2	Copy Sylink.xml to the installation files. See "Copying a Sylink.xml file to the installation files to make managed clients" on page 1107.
Step 3	Stage the administrative install image.
Step 4	Create a GPO software distribution. You should also test GPO installation with a small number of computers before the production deployment. If DNS is not configured properly, GPO installations can take an hour or more. See "Creating a GPO software distribution" on page 1103.
Step 5	Create a startup script to install Windows Installer 3.1 (or later). If your computers already meet this requirement, you may skip this step. See "Creating a startup script to install Windows Installer 3.1 or later" on page 1105.

Step	Action
Step 6	Add computers to the organizational unit. See "Adding computers to an organizational unit and installation software" on page 1106.

Table B-8 Steps for installing the client software by using Active Directory Group Policy Object *(continued)*

See "Uninstalling client software with Active Directory Group Policy Object" on page 1108.

Creating the administrative installation image

Group Policy Object installations that use Windows Installer 3.0 and lower require administrative images of the client installation files. This image is not a requirement for 3.1 and higher installations and is optional. If you do not create the administrative image, you must still copy the contents of the product disc to your computer before you install using Group Policy Object.

See "Installing clients with Active Directory Group Policy Object" on page 1101.

To create the administrative installation image

1   Copy the contents of the product disc to your computer.

2   From a command prompt, navigate to the SEP folder and type

    msiexec /a "Sep.msi"

3   In the Welcome panel, click **Next**.

4   In the Network Location panel, enter the location where you want to create the administrative install image, and then click **Install**.

5   Click **Finish**.

Creating a GPO software distribution

The procedure assumes that you have installed Microsoft's Group Policy Management Console with Service Pack 1 or later. The procedure also assumes that you have computers in the Computers group or some other group to which you want to install client software. You can drag these computers into a new group that you create.

Note: If User Account Control (UAC) is enabled, you must enable **Always install with elevated privileges** for **Computer Configuration** and **User Configuration** to install Symantec client software with a GPO. You set these options to allow all Windows users to install Symantec client software.

See

To create a GPO package

1   On the Windows Taskbar, click **Start > Programs > Administrative Tools > Group Policy Management**.

2   In the Active Directory Users and Computers window, in the console tree, right-click the domain, and then click **Active Directory Users and Computers**.

3   In the **Active Directory Users and Computers** window, right-click the Domain, and then click **New > Organizational Unit**.

4   In the New Object dialog box, in the Name box, type a name for your organizational unit, and then click **OK**.

5   In the Active Directory Users and Computers window, click **File > Exit**.

6   In the Group Policy Management window, in the console tree, right-click the organizational unit that you created, and then click **Create and Link a GPO Here**.

    You may need to refresh the domain to see your new organizational unit.

7   In the New GPO dialog box, in the Name box, type a name for your GPO, and then click **OK**.

8   In the right pane, right-click that GPO that you created, and then click **Edit**.

9   In the Group Policy Object Editor window, in the left pane, under the Computer Configuration, expand **Software Settings**.

10 Right-click **Software installation**, and then click **New > Package**.

11 In the Open dialog box, type the Universal Naming Convention (UNC) path that points to and contains the MSI package.

    Use the format as shown in the following example:

    `\\`*`server name`*`\`*`SharedDir`*`\Sep.msi`

12 Click **Open**.

13 In the Deploy Software dialog box, click **Assigned**, and then click **OK**.

    The package appears in the right pane of the Group Policy Object Editor window if you select Software Installation.

To configure templates for the package

1   In the Group Policy Object Editor window, in the console tree, display and enable the following settings:

   ■ Computer Configuration > Administrative Templates > System > Logon > Always wait for the network at computer startup and logon

   ■ Computer Configuration > Administrative Templates > System > Group Policy > Software Installation policy processing

   ■ User Configuration > Administrative Templates > Windows Components > Windows Installer > Always Install with elevated privileges

2   Close the Group Policy Object Editor window.

3   In the Group Policy Management window, in the left pane, right-click the GPO that you edited, and then click **Enforced**.

4   In the right pane, under Security Filtering, click **Add**.

5   In the dialog box, under Enter the object name to select, type **Domain Computers**, and then click **OK**.

Creating a startup script to install Windows Installer 3.1 or later

You must install Windows Installer 3.1 on the computers that contain and run earlier versions of Windows Installer. You can display Windows Installer versions by running `msiexec /?` in a command prompt. Windows Installer 3.1 or later is required for the GPO installation package. On the computers that require the installation of Windows Installer 3.1 or later, how you install it is up to you.

Note: Restricted users cannot run Windows Installer 3.1, and restricted users with elevated privileges cannot run Windows Installer 3.1. Restricted users are set with the local security policy.

One way to install Windows Installer is with a GPO computer startup script. Startup scripts execute before the GPO .msi installation files when computers restart. If you use this approach, be aware that the startup script executes and reinstalls Windows Installer every time the computer is restarted. If you install it in silent mode, however, users experience a slight delay before they see the logon screen. Symantec client software is only installed one time with a GPO.

See "Installing clients with Active Directory Group Policy Object" on page 1101.

To install Windows Installer 3.1 or later with a startup script

1   In the Group Policy Management Window, in the console tree, expand your organizational unit, right-click your package, and then click **Edit**.

2   In the Group Policy Object Editor window, in the console tree, expand **Computer Configuration > Windows Settings**, and then click **Scripts (Startup/Shutdown)**.

3   In the right pane, double-click **Startup**.

4   In the **Startup Properties** dialog box, click **Show Files**.

5   In a new window, copy the `WindowsInstaller-*.exe` file from the GPO installation file folder to the Startup window and folder.

6   Redisplay the **Startup Properties** dialog box, and then click **Add**.

7   In the **Add a Script** dialog box, click **Browse**.

8   In the **Browse** dialog box, select the Windows Installer executable file, and then click **Open**.

9   In the **Add a Script** dialog box, in the Script Parameters box, type `/quiet /norestart`, and then click **OK**.

10 In the **Startup Properties** dialog box, click **OK**.

11 Exit the Group Policy Object Manager window.

Adding computers to an organizational unit and installation software

You can add computers to an organizational unit. When the computers restart, the client software installation process begins. When users log on to the computers, the client software installation process completes. The group policy update, however, is not instantaneous, so it may take time for this policy to propagate. The procedure, however, contains the commands that you can run on the client computers to update the policy on demand.

To add computers to the organizational unit and install software

1   On the Windows Taskbar, click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

2   In the Active Directory Users and Computers window, in the console tree, locate one or more computers to add to the organizational unit that you created for GPO installation.

    Computers first appear in the Computers organizational unit.

3 Drag and drop the computers into the organization unit that you created for the installation.

4 Close the Active Directory Users and Computers window.

5 To quickly apply the changes to the client computers (for testing), open a command prompt on the client computers.

6 Type one of the following commands, and then press **Enter**.

■ On the computers that run Windows 2000, type **secedit /refreshpolicy machine_policy**.

■ On the computers that run Windows XP and later, type **gpupdate**.

7 Click **OK**.

Copying a Sylink.xml file to the installation files to make managed clients

When you install Symantec Endpoint Protection Manager, it creates a file named Sylink.xml for each client group. Symantec Endpoint Protection clients read the contents of this file to know which management server manages the client. If you do not copy this file to the installation files before you install the client software, the clients are installed as unmanaged. You should create at least one new group with the management console before you copy the file. If you do not, the Sylink.xml file causes the clients to appear in the Default group.

Note: Packages that are exported with the Symantec Endpoint Protection Manager console include a Sylink.xml file.

See "Installing clients with Active Directory Group Policy Object" on page 1101.

To copy Sylink.xml file to the installation files

1 If you have not done so, install a Symantec Endpoint Protection Manager.

See "Installing Symantec Endpoint Protection Manager" on page 95.

2 Export a Sylink.xml file from the correct client group.

See "Exporting the client-server communications file manually" on page 702.

3 Copy Sylink.xml to one of the following locations:

■ If you created an administrative installation file image, overwrite the Sylink.xml file in the folder *install_directory*\CommonAppData\Symc\Name\Version\Data\Config\. The folder *install_directory* represents the location you chose during the creation of the file image.

See "Creating the administrative installation image" on page 1103.

■ If you did not create an administrative installation file image, copy the SEP or SEPx64 folder on the product disc to a folder on your computer. Then, to create a managed client, copy the Sylink.xml file into that destination folder.

Uninstalling client software with Active Directory Group Policy Object

You can uninstall the client software that you installed with Active Directory.

See "Uninstalling the Windows client" on page 149.

To uninstall client software with Active Directory Group Policy Object

1 On the Windows Taskbar, click **Start > Programs > Administrative Tools > Group Policy Management**.

   The version of Windows that you use may display All Programs instead of Programs in the Start menu.

2 In the Group Policy Management window, in the console tree, expand the domain, expand **Computer Configuration**, expand **Software Settings**, right-click **Software Installation**, and then click **Properties**.

3 On the **Advanced** tab, check **Uninstall this application when it falls out of the scope of management**, and then click **OK**.

4 In the right pane, right-click the software package, and then click **Remove**.

5 In the Remove Software dialog box, check **Immediately uninstall the software from users and computers**, and then click **OK**.

6 Close the Group Policy Object Editor window, and then close the Group Policy Management window.

   The software uninstalls when the client computers are restarted.

Command-line options for the client

This appendix includes the following topics:

■ Running Windows commands for the client service

■ Error codes

■ Typing a parameter if the client is password-protected

Running Windows commands for the client service

You can manipulate the client directly from the command line on a Windows client computer by using the smc command for the client service. You may want to use this command in a script that runs the parameters remotely. For example, if you need to stop the client to install an application on multiple clients, you can stop and restart each client service.

The client service must run for you to use the command-line parameters, with the exception of `smc -start` parameter. The command-line parameters are not case-sensitive.

Table C-1 describes the parameters that you can run if users are members of any Windows user group.

Table C-1   Parameters that all Windows members can use

Parameter	Description
smc -checkinstallation	Checks whether the `smc` client service is installed.
	Returns 0, -3

Table C-1	Parameters that all Windows members can use *(continued)*
Parameter	**Description**
smc -checkrunning	Checks whether the `smc` client service is running. Returns 0, -4
smc -disable -ntp	Disables the Symantec Endpoint Protection firewall and Intrusion Prevent System. If the agent is password protected, type: `smc -disable -ntp -p password` See "Typing a parameter if the client is password-protected" on page 1114.
smc -dismissgui	Closes either the Symantec Endpoint Protection or Symantec Network Access Control client user interface. The client still runs and protects the client computer. Returns 0
smc -enable -ntp	Enables the Symantec Endpoint Protection firewall and Intrusion Prevent System. If the agent is password protected, type: `smc -enable -ntp -p password` See "Typing a parameter if the client is password-protected" on page 1114.

smc -exportlog	Exports the entire contents of a log to a `.txt` file.
	
	To export a log, you use the following syntax:
	
	`smc -exportlog log_type 0 -1 output_file`
	
	where:
	
	`log_type` is:
	
	■ 0 = System Log
	■ 1 = Security Log
	■ 2 = Traffic Log
	■ 3 = Packet Log
	■ 4 = Control Log
	    For example, you might type the following syntax:
	    `smc -exportlog 2 0 -1 c:\temp\TrafficLog`
	    Where:
	    `0` is the beginning of the file
	    `-1` is the end of the file
	    You can export only the Control log, Packet log, Security log, System log, and Traffic log.
	
	`output_file` is the path name and file name that you assign to the exported file.
	
	Returns 0, -2, -5

Table C-1   Parameters that all Windows members can use *(continued)*

Parameter	Description
smc -runhi	If Symantec Network Access Control is installed, runs a Host Integrity check. Returns 0
smc -showgui	Displays either the Symantec Endpoint Protection or the Symantec Network Access Control client user interface. Returns 0
smc -updateconfig	Initiates a client-server communication to ensure that the client's configuration file is up-to-date. If the client's configuration file is out-of-date, updateconfig downloads the most recent configuration file and replaces the existing configuration file, which is serdef.dat. Returns 0

Table C-2 displays the parameters you can run only if the following conditions are met:

■ The client runs Windows 2003/XP/Vista, or Windows Server 2008 and users are members of the Windows Administrators group.

■ The client runs Windows 2003/XP and users are members of the Power Users group.

If the client runs Windows Vista and the User Account Control is enabled, the user automatically becomes a member of both the Administrators and Users group. To use the following parameters, the user must be a member of the Administrators group only.

Table C-2   Parameters that members of the Administrators group can use

Parameter	Description
smc -exportconfig	Exports the client's configuration file to an .xml file. The configuration file includes all the settings on the management server, such as policies, groups, log settings, security settings, and user interface settings. You must specify the path name and file name. For example, you can type the following command: `smc -exportconfig C:\My Documents\MyCompanyprofile.xml` Returns 0, -1, -5, -6

| Table C-2 | Parameters that members of the Administrators group can use (continued) |

Parameter	Description
smc -importconfig	Replaces the contents of the client's current configuration file with an imported configuration file and updates the client's policy. The client must run to import the configuration file's contents.
	You must specify the path name and file name. For example, you can type the following command:
	`smc -importconfig C:\My Documents\MyCompanyprofile.xml.`
	Returns 0, -1, -5, -6
smc -exportadvrule	Exports the client's firewall rules to a .sar file. The exported rules can only be imported into an unmanaged client or a managed client in client control mode or mixed mode. The managed client ignores these rules in server control mode.
	You must specify the path name and file name. For example, you can type the following command:
	`smc -exportadvrule C:\myrules.sar`
	Returns 0, -1, -5, -6
	When you import configuration files and firewall rules, note that the following rules apply:
	■ You cannot import configuration files or firewall rule files directly from a mapped network drive.
	■ The client does not support UNC (Universal Naming Convention) paths.
smc -importadvrule	Adds the imported firewall rules to the client's list of existing firewall rules. These rules do not overwrite the existing rules. The client lists both existing rules and imported rules, even if each rule has the same name and parameters.
	You can import only firewall rules into an unmanaged client or a managed client in client control mode or mixed mode. The managed client ignores these rules in server control mode.
	To import firewall rules, you import a .sar file. For example, you can type the following command:
	`smc -importadvrule C:\myrules.sar`
	An entry is added to the System log after you import the rules.
	Returns 0, -1, -5, -6
smc -start	Starts the Symantec Endpoint Protection or Symantec Network Access Control client service.
	Returns 0, -1

Table C-2   Parameters that members of the Administrators group can use
                   (continued)

Parameter	Description
smc -stop	Stops the Symantec Endpoint Protection or Symantec Network Access Control client service and unloads it from memory. Returns 0, -1

To run Windows commands for the client service:

◆   Do one of the following tasks:

■   Click **Start** > **Run**, and type the command.

■   In a DOS prompt window, type the installation path to the smc service before the command.
For example, on a 64-bit Windows system, type:

```
C:\Program Files (x86)\Symantec\Symantec Endpoint
Protection\smc.exe
```

Error codes

Table C-3 displays the error codes that the `smc` command returns when the required parameters are invalid or missing.

Table C-3   Smc error codes

Error code	Description
0	Command was successful.
-1	User is not in the Windows Administrators or Windows Power Users group. If the client runs Windows Vista, the user is not a member of the Windows Administrators group.
-2	Invalid parameter. You may have typed the parameter incorrectly, or you may have added an incorrect switch after the parameter.
-3	`smc` client service is not installed.
-4	`smc` client service is not running.

Table C-3   Smc error codes *(continued)*

Error code	Description
-5	Invalid input file. For example, the `importconfig`, `exportconfig`, `updateconfig`, `importadv`, `exportadvrule`, and `exportlog` parameters require the correct path name and file name.
-6	Input file does not exist. For example, the `importconfig`, `updateconfig`, and `importadvrule` parameters require the correct path name, configuration file name (.xml) or firewall rules file name (.sar).

Typing a parameter if the client is password-protected

You can set up password-protection on the client if you or another user either stops the client service or imports or exports the configuration file. You must type the password if the client is password-protected for the following parameters:

-stop	The client asks for a password before you or the user stops the client.
-importconfig	The client asks for a password before you can import the configuration file.
-exportconfig	The client asks for a password before you can export the configuration file.

See "Password-protecting the client" on page 245.

Note: The password is limited to 15 characters or less.

To type a parameter if the client is password-protected

1 On the client computer, on the taskbar, click **Start > Run**.

2 In the **Run** dialog box, type **cmd**

3   In the Windows MS-DOS prompt, type either one of the following parameters:

smc *-parameter* -p *password*

smc -p *password* *-parameter*

Where:

parameter is -stop, -importconfig, or -exportconfig.

password is the password you specified in the console.

For example, you can type either of the following syntax:

smc -exportconfig c:\profile.xml -p *password* or

smc -p *password* -exportconfig c:\profile.xml

4   Close the command prompt.

Command-line options for the Virtual Image Exception tool

This appendix includes the following topics:

■ vietool

vietool

vietool – Runs the Virtual Image Exception tool

SYNOPSIS

vietool.exe *volume*: --generate|clear|verify|hash [options ...]

DESCRIPTION

The vietool command marks the base image files on the volume that you specify by adding an attribute.

OPTIONS

--generate

    Runs the Virtual Image Exception tool on all files on the volume specified. You cannot use this option with --clear.

    For example: vietool c: --generate

--verify

    Verifies that the Virtual Image Exception is set on all files on the specified volume. You cannot use this option with --clear.

    For example: vietool c: --verify

--clear

    Removes the Virtual Image Exception on all files on the volume specified.

    For example: vietool.exe c: --clear

    To delete a specific file: vietool.exe c:\Users\Administrator\target.file --clear

    You can use a fully qualified path in place of the volume identifier to clear the Virtual Image Exception on a single file or the contents of a folder. Only one file name, folder name, or volume identifier per command line is allowed. You cannot use this command with --generate, --verify, or --hash.

    You must restart the client after you run the --clear command.

--hash

    Generates the hash value on all files on the volume specified.

The client shares the hash value with the Shared Insight Cache. The Virtual Image Exception tool does not generate the hash value unless it needs it. You cannot use this option with `--clear`.

For example: `vietool.exe c: --generate --hash`

`--volume arg`

Specifies the volume the tool scans.

This option can be a file when you use the `--clear` option. You must specify the volume, and it can be specified either with the volume flag or alone. For example, with the flag `vietool.exe --volume c: --generate`, or alone `vietool.exe c: --generate`.

`--verbose`

Outputs to the console the maximum amount of program execution information.

`--stop`

Stops on the first error that the tool encounters. Otherwise the tool writes error information to the console and continues.

`--help`

Displays this help message.

Appendix E

Syntax for custom intrusion prevention signatures and application control rules

This appendix includes the following topics:

- Regular expressions in Symantec Endpoint Protection Manager

- About signature syntax and conventions

- Protocol type arguments

- TCP protocol arguments

- UDP protocol arguments

- ICMP protocol arguments

- IP protocol arguments

- Msg arguments

- Content arguments

- Optional content arguments

- Case-sensitivity

- HTTP decoding

- Offset and depth

- Streamdepth arguments

- Supported operators

■ Sample custom IPS signature syntax

Regular expressions in Symantec Endpoint Protection Manager

You can use regular expressions in the IPS signature content and application control rules. By default, the regular expressions are case-sensitive.

For IPS, regular expressions use the following format:

```
regexpcontent="string value" (offset , depth)opt
```

offset	Specifies the start of the bytes in the packet data, from which the IPS engine matches the signature pattern.
depth	Specifies the length of the packet data in which the IPS engine matches the signature pattern.
opt	Includes the C and the H options. ■ The C option makes the expression not case-sensitive. ■ The H option specifies HTTP decoding. ■ If there is no option, the entire data packet is matched.

For both IPS and application control, regular expressions support the following characteristics:

■ Multiple regexpcontent

■ Case-sensitivity

■ Binary format. The format is \x or \X with two Hex digits, like \xA9.

Table E-1   Syntax for regular expressions

Symbol	Description
Character	Matches itself, unless it is one of the following special characters (metacharacters): . \ [ ] * + ^ $
.	Matches any character and means one or more.

Table E-1   Syntax for regular expressions *(continued)*

Symbol	Description
\	Matches the character following it, except when followed by: ■ A left round bracket or a right round bracket. ■ A left angle bracket or right angle bracket. ■ A digit from 1 to 9. The \ character is used as an escape character for all other metacharacters as well as itself. When it is used in a set ([4]), the \ character is treated as an ordinary character.
[set] [^set]	Matches one of the characters in the set. If the first character in the set is "^", it matches a character NOT in the set, i.e., it complements the set. A shorthand S-E is used to specify a set of characters S up to E, inclusive. The special characters "]" and "-" have no special meaning if they appear as the first chars in the set. For example: ■ [a-z]: Matches any alphabetic character ■ [^]-]: Matches any character except] and - ■ [^A-Z]: Matches any character except alpha character ■ [a-z A-Z]: Matches any alphabetic character. It is the same as [a-z] or [A-Z]
*	Any regular expression from [1] to [4] followed by a closure character (*) that matches zero or more matches of that form.
+	Same as *, except that + matches one or more
\(*form*\)	A regular expression in supported syntax, enclosed as \(*form*\), matches whatever *form* matches. The enclosure tags the form to be used with \<*digit from 1 to 9.*> for pattern substitution. The tagged forms are numbered in sequence starting at the beginning of the syntax. For example: ■ \(xxx\)[1-3] matches xxx1 or xxx2 or xxx3

Table E-1 Syntax for regular expressions *(continued)*

Symbol	Description
\<*digit from 1 to 9.*>	Matches whatever a previously tagged regular expression \(*form*\) matched. The digit indicates which tagged form to match. In the first example here, \(xxx\) is tagged as 1. In the second example, \(yy\) is tagged as 1, (zz\) is tagged as 2. ■ \(xxx\)[1-3]\1 matches xxx1xxx or xxx2xxx or xxx3xxx ■ \(yy\)X\(zz\)[1-3]\2\1 matches yyXzz1zzyy or yyXzz2zzyy or yyXzz3zzyy
\< \>	A regular expression that starts with \< and/or ends with \> restricts the pattern matching to the beginning of a word and/or the end of a word. A word is defined to be a character string that begins and/or ends with the characters A-Z a-z 0-9 and _. It must also be preceded or followed by any character outside those mentioned. For example, the syntax: .*\<Symantec.\>.* matches ...ABC Symantec 123....
N/A	A composite regular expression xy where x and y are in the form [1] to [10] matches the longest match of x followed by a match for y.
N/A ^ $	A regular expression that starts with a ^ character and/or ending with a $ character, restricts the pattern matching to the beginning of the line, or the end of line [anchors]. Elsewhere in the pattern, ^ and $ are treated as ordinary characters.

About signature syntax and conventions

When you write the content for each IPS signature, you must use the following syntax:

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

You must begin each signature with the keyword `rule`, followed by the protocol type argument, protocol options, IP protocol options, msg arguments, and content arguments. The optional arguments are enclosed in square brackets. Type only the information within the brackets; do not type the brackets. Arguments that are followed by an ellipsis may be repeated. You provide the information for the arguments, by using the supported operators and the regular expressions.

See "Protocol type arguments" on page 1125.

See "IP protocol arguments" on page 1129.

See "Msg arguments" on page 1132.

See "Content arguments" on page 1133.

See "Supported operators" on page 1136.

See "Regular expressions in Symantec Endpoint Protection Manager" on page 1122.

Protocol type arguments

This part of the signature defines the protocol type by using the following syntax:

```
protocol-type
```

where `protocol-type` is one of the following parameters:

- `tcp`
- `udp`
- `icmp`

The protocol type must immediately follow the word `rule`.

For example:

```
rule udp
```

Each `tcp`, `udp`, and `icmp` protocol type supports its own set of optional arguments.

See "TCP protocol arguments" on page 1125.

See "UDP protocol arguments" on page 1127.

See "ICMP protocol arguments" on page 1128.

TCP protocol arguments

For additional details on the TCP protocol, refer to RFC 793.

Table E-2   TCP protocol arguments

Attribute	Description	Syntax

source	Source TCP port	`source operator (value)`
		
		where `value` is an unsigned 16-bit number from 0 to 65535.
		
		Example:
		
		`source=(180,2100)`
		
		The value must be enclosed in parentheses. A value of 0 (zero) indicates all ports.
		
		You can specify a range of ports by using a dash between two port values (for example 3-5 is ports 3, 4, and 5). Multiple ports can be specified by separating them with commas.

dest	Destination TCP port	`dest operator (value)` where value is an unsigned 16-bit number from 0 to 65535. For example: dest=(120,125) value must be enclosed in parentheses. A value of 0 (zero) indicates all ports. A range of ports can be specified by using a dash between two port values (for example 3-5 is ports 3, 4, and 5). Multiple ports can be specified by separating them with commas.

Table E-2   TCP protocol arguments *(continued)*

Attribute	Description	Syntax

tcp_flag	TCP flags present in the packet	`tcp_flag operator flag|[flag]...`
		
		 where `flag` is one of the following parameters:
		
		 ■ fin: end of data
		 ■ syn: synchronize sequence numbers
		 ■ rst: reset connection
		 ■ psh: push function
		 ■ ack: acknowledgement field significant
		 ■ urg: urgent pointer field significant
		 ■ 0: match all flags
		
		 For example:
		
		 `tcp_flag&ack|ps`
		
		 Most tcp_flag tests use the & (bitwise and) operator as a mask (meaning that a packet must have the specified flags set but can also have other flags set).
		
		 You can specify multiple flags in a test by placing a pipe character
			between the flags.

window	TCP window size	`window operator size`
		
		 where `operator size` is an unsigned 16-bit number from 0 to 65535.
		
		 For example:
		
		 `window=16384`

UDP protocol arguments

For additional details on UDP protocol, refer to RFC 768.

Table E-3   UDP protocol arguments

Attribute	Description	Syntax

source	Source UDP port	`source operator (value)`
		
		where `value` is an unsigned 16-bit number from 0 to 65535.
		
		For example:
		
		`source=(180,2100)`
		
		The value must be enclosed in parentheses. A value of 0 (zero) indicates all ports.
		
		A range of ports can be specified by using a dash between two port values (for example 3-5 is ports 3, 4, and 5). Multiple ports can be specified by separating them with commas.

dest	Destination UDP port	`dest operator (value)`
		
		where `value` is an unsigned 16-bit number from 0 to 65535.
		
		For example:
		
		`dest=(120)`
		
		The value must be enclosed in parentheses. A value of 0 (zero) indicates all ports.
		
		A range of ports can be specified using a dash between two port values (for example 3-5 is ports 3, 4, and 5). Multiple ports can be specified by separating them with commas.

ICMP protocol arguments

Refer to RFCs 792 and 1256 for detailed descriptions of valid ICMP protocol type and code combinations.

Table E-4   ICMP protocol arguments

Attribute	Description	Syntax
type	ICMP protocol type	`type operator value` where `value` is an unsigned 8-bit number from 0 to 255. For example: `type=0`

code	ICMP protocol type	`code operator value`
		
		where `value` is an unsigned 8-bit number from 0 to 255.
		
		For example:
		
		`code<=10`

IP protocol arguments

The IP protocol arguments are independent of the protocol type arguments and are valid for the TCP, UDP, and ICMP protocol types.

For additional details on IP protocol, refer to RFC 791.

Table E-5   IP protocol arguments

Attribute	Description	Syntax

saddr	Source IP address	`saddr=(value/CIDR)`
		
		where:
		
		■ `value` is a standard 32-bit IP address or the variable $LOCALHOST, which specifies the IP address of the client computer.
		■ `CIDR` is a classless inter-domain routing notation that indicates how many bits are used for the network prefix.
		
		For example:
		
		`saddr=(127.0.0.0/25)`
		
		Here, 25 bits are used to identify the unique network and the remaining bits that identify the host.

daddr	Destination IP address	`daddr=(value/CIDR)`
		
		where:
		
		■ `value` is an IP address or the variable $LOCALHOST, which specifies the IP address of the computer that runs the client.
		■ `CIDR` is a classless inter-domain routing notation that indicates how many bits are used for the network prefix.
		
		For example:
		
		`daddr=(128.0.0.0/4)`
		
		Here, four bits are used to identify the unique network and the remaining bits that identify the host.

Table E-5 IP protocol arguments *(continued)*

Attribute	Description	Syntax

tos	Type of service flag present in the packet	`tos operator value`
		
		where `value` is a numeric constant in a decimal, hexadecimal, or octal format.
		
		For example:
		
		`tos=0x4`
		
		To view valid IP tos values, see Table E-6.
		
		To test for multiple IP tos values in a packet, the tos argument should be the sum of the values that are to be tested. Typically, the operator is either = or &. These flags cannot be combined by using the pipe character (|) as in tcp_flags.

tot_len	Total length of the packet	`tot_len operator value`
		
		where `value` is a 16-bit number from 0 to 65535 that specifies the total length of packet.
		
		For example:
		
		`tot_len>1445`
		
		When you specify the value, the rule protocol-type must be considered to properly calculate the length to be tested. To aid in calculating the tot_len for each of the supported protocol types, their header lengths are as follows:
		
		TCP: 20-60 bytes
		
		UDP: 8 bytes
		
		ICMP: 8-20 bytes

Table E-5 IP protocol arguments *(continued)*

Attribute	Description	Syntax
ttl	Time-to-live (TTL) of the packet	`ttl operator value` where `value` is an 8-bit value from 0 to 255 that specifies the time-to-live characteristic of the packet.
ip_flag	Fragmentation offset value of the packet	`ip_flag operator value` where `value` is a 13-bit value that specifies the fragmented offset value in the packet. IP fragmentation offsets occur on 8-byte boundaries; therefore, each bit value in the fragmentation offset represents three bits.

Table E-6 Valid IP tos values

Dec	Hex	Option
2	0x2	Minimize monetary cost
4	0x4	Maximize reliability
8	0x8	Maximize throughput
24	0x18	Minimize delay

Msg arguments

When an IPS signature successfully matches packet content with the rule's test conditions, the message is specified in the msg argument. The msg argument appears in the Security Log on both the client and the server. Only one msg argument can be included in each IPS signature.

Syntax:

```
msg="alert message"
```

The alert message must be enclosed in double quotation marks and cannot contain punctuation. Single quotation marks are not allowed. The purpose of the alert message is to let you easily identify an event in your network by reviewing the

Security Log. Therefore, all IPS signatures must contain concise yet descriptive alert messages within the msg argument.

Example:

```
msg="IIS Unicode Transversal Vulnerability"
```

Content arguments

The content argument specifies a pattern to look for within a packet. The content argument can appear multiple times in an IPS signature. The content value must be enclosed in double quotation marks (" "). Single quotation marks (' ') are not allowed.

Syntax:

```
content="value"
```

where value is a pattern that is specified as a string literal or a binary literal that must be enclosed in quotation marks.

A string literal is a group of consecutive characters, including spaces. A string can contain any characters except a quotation mark ("), backslash (\), or newline character escape sequence (\n). Example:

```
content="system32"
```

A binary literal is a group of consecutive bytes expressed in hexadecimal format, where the escape sequence \x precedes each byte. Example:

```
content="\x04\x20\x20\x20\xBF"
```

The following example specifies the content as the binary literal "\x04\x20\x20\x20\xBF".

String literals can be combined with binary literals to create complex patterns. Example:

```
content="\x0DLocation\x3A"
```

Optional content arguments

You can use additional optional content arguments to further qualify the content in the following ways:

■ Case-sensitivity

■ HTTP decoding

■ Depth and offset

Case-sensitivity

You can specify an optional C case-sensitivity flag on each content argument. When the flag follows a content argument, the pattern that is contained in the content argument matches only if the case of the characters in the string matches the case of the data in the packet.

For example, you can use the following syntax:

```
content="value"C
```

```
content="\x0DLocation\x3A"C
```

HTTP decoding

You can use the optional HTTP H decoding flag in each content argument. If you use the H HTTP decoding flag, encoded characters are converted into a binary literal before they try a pattern match. You can also use the HTTP H after a C case-sensitivity flag. HTTP URIs use encoded characters. When the pattern match is attempted and normalized, the normalized data is compared to the binary or the string literal in the content argument. Under most circumstances, the H flag is used only for the TCP rules that relate to an application that uses the HTTP protocol.

For example, you can use the following syntax:

```
content="value"H
```

```
content="\x6f\x6e\x4c\x6f\x61\x64\x3d\x22\x61\x6c\x65\x72\x74\x28"H
```

Offset and depth

You can use the offset value and a depth value as optional arguments in the content. The offset value is specified first, followed by the depth value.

For example, you can use the following syntax:

```
content="value"(offset,depth)
```

Syntax	Description
value	A pattern that is specified as a string literal or a binary literal that must be enclosed in quotation marks.

Syntax	Description
offset	A positive integer in decimal notation.
	The offset specifies an alternative location to begin a pattern match. The offset also specifies how many bytes to skip before the signature tries to pattern match.
	When an offset argument is not present or has a value of 0, the content argument pattern tries to find a match. The pattern tries to match the content at the beginning of the packet payload or the portion of the packet following the protocol header for the first content argument. Each successive content argument automatically begins to test for pattern matches that follow the end of the previous successful pattern match.
depth	A positive integer in decimal notation. The depth specifies the maximum number of bytes to search when trying to match a pattern in a content argument.
	When a depth argument has a value of 0, the pattern that is contained in the content argument tries to find a match from the offset to the end of the packet. The depth argument value cannot be smaller than the number of bytes that are specified as the pattern to match within the argument of the content argument.

```
content="\x04\x20\x20\x20\xBF"(4,5)
```

This example skips four bytes forward from the previous pattern match or from the beginning of the packet payload and compares the next five bytes with the binary literal that is contained in the content argument.

Streamdepth arguments

You can use the streamdepth argument to limit the length of the stream in which the intrusion prevention rule checks for a signature. You might want to use streamdepth to improve the performance of your custom intrusion prevention rules. The streamdepth argument is optional.

Syntax:

```
streamdepth=value
```

For example, you might suspect that a signature exists in the first 10KB of a 1MB stream. You can use the following syntax:

```
streamdepth=10240
```

On the file download, the intrusion prevention rule with this streamdepth value stops checking for the signature after 10KB. Since you limit the checking, the download performance is improved.

If you set streamdepth to 0, intrusion prevention applies the rule to the entire stream.

Supported operators

Many arguments in the signature syntax require an operator that indicates the type of test that is to be performed to check for this type of attempt.

Table E-7 describes the supported operators.

Table E-7   Supported operators used in IPS signatures

Operator	Description
<	less than
>	greater than
=	equal to
&	bitwise and
	In the signature library, the ampersand character & is sometimes represented using its HTML equivalent &
<=	less than or equal to
>=	greater than or equal to

Sample custom IPS signature syntax

You can create sample custom IPS signatures to detect an attempt to access and download MP3 files through a Web browser or FTP.

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.

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.

When you create a custom IPS signature, you must type the content of the signature by using the following format:

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

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.

Web browsers use the HTTP GET command to download MP3 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 signature syntax 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. If you do not know the name of a particular 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.

See "Regular expressions in Symantec Endpoint Protection Manager" on page 1122.

The content of the HTTP signature contains the following syntax:

```
rule tcp, dest=(80,443), saddr=$LOCALHOST,
msg="MP3 GET in HTTP detected",
regexpcontent="[Gg][Ee][Tt] .*[Mm][Pp]3 .*"
```

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",
regexpcontent="[Rr][Ee][Tt][Rr] .*[Mm][Pp]3\x0d\x0a"
```

Table E-8 explains the syntax for the HTTP signature and the FTP signature.

Table E-8 HTTP signature and FTP signature syntax

Use the following syntax	To perform the following task

For the HTTP signature:
 	
`rule tcp dest=(80,443)`
 	
For the FTP signature:
 	
`rule tcp dest=(21)`
	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 you 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.

For the FTP signature: `tcp_flag&ack`	Reduces the false positives.
`saddr=$LOCALHOST`	Makes sure that the request originates on the host.

For the HTTP signature:
 	
`msg="MP3 GET in HTTP"`
 	
For the FTP signature:
 	
`msg="MP3 GET in FTP"`
	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.

For the HTTP signature:
 	
`regexpcontent="[Gg][Ee][Tt] .*[Mm][Pp]3 .*"`
 	
For the FTP signature:
 	
`regexpcontent="[Rr][Ee][Tt][Rr] .*[Mm][Pp]3\x0d\x0a"`
	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.
	
	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.
	
	The string is written so that the text can be case-insensitive.

Index